Helping you move from fear to fearlessness with these IBM i security features

By Robert Andrews | 3 minute read | November 27, 2019

Given the reality of constantly evolving security threats, IBM works to offer our clients security rich computing environments. We do this using an approach to add security at all layers, from the hardware to the operating systems and enterprise-wide monitoring tools. IBM i, the choice for an integrated operating system on IBM Power Systems, is no exception. In this post, I'll cover some of the valuable security technologies for IBM i that help keep you safe in today's threat-filled IT landscape.

Reduce insider threats

A company's employees are one of its most valuable assets. However, they can also be one of the biggest threats. This is because they have access to another major asset — your data. When I'm performing security assessments, one of the biggest issues I see is that users often have a much higher level of authority to access systems and data than their job requires. This has the potential to threaten your customers' data and can lead to system outages and downtime caused by the permissioned user. The problem has always been knowing just what level of authority is correct — not too much, which increases risk, and not too little, which could cause errors and delays.

Authority Collection is a feature of IBM i that allows a system administrator to trace the logic of authorization decisions to determine the “just right” level of authority. By using Authority Collection, a security officer can see the level of access required or requested, the actual level the user has, and the source of that authority. This way, if a user has a higher level of authority than is needed, the security officer can reduce it to minimize the threat.

Learn more about Authority Collection.

Keeping up with krypto

Most IT security professionals understand the need to keep our communications secure using data in flight encryption via Transport Layer Security (TLS). An important factor in TLS is the algorithm used for encryption. Today, the most common ones are based on factoring large numbers into primes. However, with the Quantum computing development effort, this style of encryption could be at risk in the future. New types of encryption that are thought to be more quantum safe, such as Elliptic Curve Cryptography (ECC), have been developed. IBM i includes these new, advanced algorithms to help keep your communications safe. Make sure you’re taking advantage of this.

Learn more about TLS.

Sending out an SOS

One of the major strengths of IBM i is its robust audit and logging facilities. As enterprises move to consolidated, centralized security information and event management (SIEM) tools like IBM Security QRadar and Splunk, IBM i has provided methods to translate our internal logs to the common messaging format of Syslog. The issue remains how to effectively move them off the local system and get them into the SIEM tool. To help complete the picture, IBM Systems Lab Services introduced the IBM i Syslog Reporting Manager. This asset allows system administrators to selectively filter which entries are extracted and then sent to a SIEM tool in near real time. Once the logs arrive at the central SIEM, it can apply rules to take actions based on the messages.

Ransomware safety

One final note on the recent outbreak of ransomware. While ransomware will not run directly on IBM i, your system still may be at risk from a mapped network drive. Once ransomware infects a PC, it will attempt to encrypt not only the local drives' contents but any attached network drive as well, including IBM i. To reduce the risk to IBM i, do not share the root of the integrated file system (IFS), and make sure as many shares as possible are set to read only.

Help is available!

The IBM i Lab Services Security Team is here to help you move from fear to fearlessness. Want to better understand the security posture of your system? Looking to set up new features such as TLS or single sign-on? We can help! Contact Lab Services to learn more about our services and tools.

From: https://www.ibm.com/blogs/systems/helping-you-move-from-fear-to-fearlessness-with-these-ibm-i-security-features/