RAZ-LEE

EBOOK

Understanding your IBM i security needs

Table of Contents

IBM i Security and Reliability is Best of Breed

The IBM i is among the most secure and reliable systems used in business today. It is often considered a fortress. It has no known viruses. Extremely few breaches have been reported in comparison to Windows or UNIX-based servers. While businesses use fewer IBM i systems than Windows PCs and servers, many industries have a large number of them around the world, such as banking and finance institutions, manufacturing facilities, and retailers.

The banking and finance sector alone is attractive enough to attract hackers and viruses. There certainly isn't a lack of people who have worked with the IBM i or its earlier AS/400, System i, and iSeries systems. Many of them would have developed the technical skills to cause problems. Something more is at the heart of the IBM i's reputation for reliability and security.

Security Costs of Opening the ‘i’ to New Technologies

The IBM i was designed for security. Because of its reputation as a fortress, system security is often overlooked, leaving valuable company data vulnerable to breach and exposure. In the past, when the systems were isolated, connected only to dedicated terminals, they seemed impenetrable. Today, everything is connected. Many activities that were previously impossible in the closed AS/400 environment are now easily carried out remotely, such as initiating commands, installing or activating programs, updating or erasing data, and moving or copying files to and from IBM i servers. To harness and use the power of IBM i, the servers need to be connected to networks and, ultimately, the world.

From the first moment that an AS/400 connected to a PC, the systems became vulnerable to attack. A torrent of new weaknesses appeared as the IBM i became a popular server, hosting a variety of different systems. The systems have to be protected as these and other issues continue to arise.

> “Because of its reputation as a fortress, system security is often overlooked, leaving valuable company data vulnerable to breach and exposure.”

The IBM i is Highly Secure

Even with these growing challenges over the years, the security and stability of the IBM i remain legendary. This leads IBM i shops to continue to view the system as even more invincible than it actually is. IBM i shops often don't take the steps needed to protect the systems against the serious, real risk of these attacks and security failures.

While the systems could be protected by completely disconnecting them from networks, no one would be able to use the full capacity of the IBM i for what it does best. In the real world, where everything is connected, each organization has to define and implement its policies toward

- System Security
- Access Controls for Objects
- Protection against Malware and Viruses
- Encrypting Data and Interfaces, and
- Internal and Regulatory Auditing

It is still possible to keep the IBM i secure. This requires continual management of the IBM i's inherent security vulnerabilities.

System Security

Access Control of Objects

Anti-Virus Protection

Encryption

Audit

IFS: IBM i Inherent Security Weakness

Attackers who know even a little about the IBM i know that the Integrated File System (IFS) is its weakest point. Introduced over twenty-five years ago, it overlaid an industry-standard directory structure on the existing QSYS library system. The IBM i could store and manage the same file types as other network servers, using standard methods and pathnames.

Since the IFS is built on top of the IBM i's essential QSYS library, PCs see the library as a regular directory. That makes it dangerously simple to access and modify. Someone running a malicious program on a connected PC, knowingly or not, could copy and delete data and objects anywhere within it. They could even damage programs or the IBM i's operating system itself.

And it does not stop there. It is surprising what is on the IFS and what could be damaged.

Vulnerabilities - Not Just The IFS

IBM i security problems aren't limited to the IFS. People who have access to the system and know it well can steal data and harm the system. These aren't only outsiders who have sniffed out credentials for access. Legitimate users could, either by going rogue or through honest accidents, access areas and objects that they shouldn't be able to reach and can damage everything that is not secured.

User Privileges
(Errors)

Technical Team
(Errors)

Illicit Intent

IBM i’s Integrated Security Not Enough

The threat of Cyber-attacks against the IBM i is very real. Cyber-attacks have been growing at an alarming rate – in volume, sophistication and impact..

IBM i’s integrated security does not provide a satisfactory security solution for this new interconnected world – it only includes a security infrastructure, leaving it to professional security solutions to turn this infrastructure into a manageable and beneficial tool for managers and auditors.

There are three main security areas that need to be reinforced in the IBM i:

- Cyber & Security
- Auditing & Monitoring
- Risk & Security Assessment

> “The threat of Cyber-attacks against the IBM i is very real. Cyber-attacks have been growing at an alarming rate – in volume, sophistication and impact.”

Cyber & Security Needs

NETWORK SECURITY

- TCP/IP was added to the Menu based system
- The Environment has changed – New risk appeared
- Access are not truly secured as :
  - Security was Enabled, but Not Provided
  - There is no log
- ODBC, FTP, etc. are well known & commonly used

DATA PROTECTION

- Expediting compliance with industry and government regulations
  - GDPR, PCI-DSS, HIPAA, FDA 21 CFR Part 11, and other regulations
- Fortification of business-critical data
- Segregate the way data is displayed:

Clear text	5201	1234	5554	0830
Masked	* * * *	* * * *	* * * *	0830
No data	-------------------------			

Cyber & Security Needs (cont.)

ADVANCED THREAT PROTECTION

- Hackers use a variety of tools to launch attacks, including malware, ransomware, exploit kits, and other methods
- IBM i is no longer an isolated system but connected to other databases through networked systems and connectivity
- IBM i is vulnerable to existing and emerging threats

AUTHORITY & USER MANAGEMENT

- Control user privileges
- Protect sensitive data from those who shouldn't have access
- Mandatory Security Regulations
  - GDPR, PCI-DSS, HIPAA, SOX and other regulations
- Audit trail of access to data

Auditing & Monitoring Needs

DATABASE MONITORING

- To ensure IT systems are reliable, secure and not vulnerable to computer attacks.
- To reduce risks of data tampering, data loss or leakage, service disruption, and poor management of IT systems.
- Mandatory Security Regulations
  - GDPR, NIS Directive, HIPAA, SOX
- Event and User Activity Tracking
- External auditor's demands
- Internal security policies

TRACING DB ACTIVITY

- To answer auditor's demands
- To check application DB activities
- To report changes of information across time
- To understand activities related to a single person/account/order… by multiple dimensions
- To answer many questions such as: Who made this change? When was it done? By which program?
- To maintain integrity of sensitive data from tampering and loss
- To comply with mandatory Security Regulations
  - GDPR, PCI-DSS, HIPAA, SOX, FDA 21 CFR Part 11, and other regulations

Risk & Security Assessment

Do you know how effective your IBM i security is?

In today's market, corporate scandals have generated high regulatory involvement by the government. New laws are being continually enacted to enhance the quality of corporate reporting. New government regulations such as the Sarbanes-Oxley Act (SOX), GDPR, HIPAA and PCI have significantly impacted business and various other industries. Organizations need to know how well their systems comply with mandatory industry and government regulations. This requires a comprehensive diagnosis of their security configurations, pinpointing the location of sensitive data, the security of native OS/400 objects, and where missteps such as granting excessive user authority can lead to security risks. For continual assessment and enforcement, organizations need to automate tasks handling security administration and compliance, delivering real-time alerts when they detect security threats, integrated with SIEM products for forensic analyses of these events.

Assess, Protect, & Detect with iSecurity

Raz-Lee's iSecurity Assessment is a non-intrusive solution that easily identifies the security risks present in the IBM i. It provides an in-depth analysis of the full scope of the IBM i server's security strengths and weaknesses, pinpointing the security risks that need to be addressed. It delivers a detailed report, grading each facet of IBM i security, with full explanations.

iSecurity solutions enable companies to effortlessly achieve data safety and compliance.

About Raz-Lee Security

Raz-Lee Security, headquartered in Nanuet, New York, is a leading independent cybersecurity and compliance solutions provider for IBM's IBM i (AS/400) midrange computers. With more than 35 years of expertise and customers in over 40 countries, Raz-Lee's flagship iSecurity suite guards organizations against insider threat and unauthorized external access to business-critical information hosted on their IBM i. The company continues to develop and market cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

www.razlee.com