IAM FOR IBM i, EXPLAINED

GRANT THE RIGHT ACCESS FOR THE RIGHT PURPOSE

CSI
YOUR PERPETUAL EDGE

DO NOT LET USER RISKS SLIP UNDER YOUR BUSINESS' RADAR.

Where is the risk?

Ignoring IBM i security threats simply because it can seem like issues go unreported is not a robust strategy. So, let's talk about your users. Rarely is proper role-based access management already in place on IBM i servers.

Historically, user management has not been policed, often resulting in unauthorised permissions falling into the wrong pair of hands. When user access goes unmanaged, there is a larger than expected risk to your server and your data. Whether through human error, or a breach, user credentials can be abused to extort, steal, ransom or encrypt the likes of financial, transactional or other sensitive data. With so many users going remote, do you really know who is logging on?

Did you know... most compliance frameworks mandate or recommend Two- or Multi-Factor Authentication (2FA/MFA) for highly privileged users and access to cloud environments.

TRUSTED TECHNOLOGY PARTNERS

FORTRA™ IBM i IBM® Platinum Partner

WHAT ACTIONS SHOULD BE TAKEN?

Trying to manage Identity & Access Management (IAM) with a policy and a process uses resource time that could better be used elsewhere. A service to manage your users will alleviate that pain leaving your environment more secure and your resources time to concentrate on other projects.

01 / GIVE USERS WHAT THEY NEED.

Extend privileged access management to IBM i. You can even control powerful users, such as programmers, to ensure key users have the flexibility they require.

- Tightly monitor what a user is doing
- Limit the number of privileged users on your system
- Employ 'separation of duties' for best practice
- Satisfy auditors and prevent conflicts of interest

02 / CONTORL ACCESS FROM OUTSIDE THE ENVIRONMENT.

Many IBM i shops do not have any intrusion detection and prevention solutions on IBM i to stop and audit authorised and unauthorised access.

- You should ensure that there is essential security in place by putting Exit Point Management at the doors to your server
- Exit Point Manager will provide protection against unauthorised access and report on all access
- It will block unauthorised access, alert real-time and report

03 / MULTI-FACTOR AUTHENTICATION.

Don't trust login and password only, apply multi-factor authentication to something you know (login and password), something you have and something you are.

- Biometrics, Yubi keys, one-time passwords add a layer of additional validation
- Integration with Duo, AWS NPS and other authentication such as PingID

04 / REGULAR ACCESS REVIEW.

Once you have your layers of identity validation in place you should monitor the compliance against your access policy and any compliance and regulatory frameworks for your industry sector.

- Report against regular access reviews
- Notify when a user goes outside your policy
- Run regular login and password management processes
- Grant managerial reviews of users for verification

Get a free non disruptive security scan today!

WHAT IS THE BENEFIT TO YOUR ORGANISATION ?

By applying the principle of Zero Trust with a robust IBM i access policy you can prevent insider threats on your IBM i; thereby reducing the possibility of unplanned downtime, data breach and compliance infringement by verifying users every time they request access and operating the principle of least privilege. It saves your organisation time and money!

You will have a defined access policy that can be evidenced and audited – it is a demonstrable step on your IBM i cybersecurity maturity that you can share with business partners.

NEXT STEPS...

CSI security services will help you set-up your IAM for the IBM i by providing services underpinned by Fortra Powertech IBM i security solutions to address the pain of access management and provide the overseeing of the process and regular reporting to your business.

The solutions which form these service elements are:

- Powertech Authority Broker
- Powertech Exit Point Manager
- Powertech Multi-factor Authentication for IBMi
- Powertech Password Self-Help For IBM i
- Powertech Compliance Monitor

CSI Ltd Head Office

CSI House
2940 Trident Court
Birmingham Business Park
Solihull Parkway
Birmingham B37 7YN

CONTACT INFO

+44 (0) 800 1088301
info@csiltd.co.uk
www.csiltd.co.uk