SECURING IDENTITY ACCESS MANAGEMENT (IAM) PLATFORMS

Introduction

IAM solutions are ever more popular and rightly so. They provide a centalised platform to control user access to an organisation's technical infrastructure. However, as with any application, programme, or platform, it is vital to assess and evaluate the associated risks in order to develop a strategy to mitigate against them and ensure stringent cyber security standards are upheld. This document outlines some of these risks and provides suggestions on how to address them.

TELESOFT

What is IAM?

Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times and for the right reasons. IAM addresses the need to ensure appropriate access to resources across increasingly diverse technology environments and to meet increasingly rigorous compliance requirements.

Some key components of an IAM program include:

- Directory services - Stores user profile data and credentials for authentication
- Identity provisioning - Creates, manages and governs user identities and access
- Access management - Grants authenticated users the appropriate access to resources
- Access certification - Reviews and approves user access rights periodically

Examples of IAM Platforms

- Okta
- Microsoft Active Directory
- IBM Security Identity Manager
- Oracle Identity Management

The Problem

As more organisations move to cloud-based networks, it is vital that cyber security standards are upheld. IAMs are a great way to centralise cloud-based applications into one platform. Unfortunately, this also means that if your organisations IAM platform is hacked, it provides cyber criminals with access to significant amounts of sensitive data.

For example, the September MGM attack initiated after the attacker was granted the ability to change the password for an account linked to the organisation's Okta, a popular IAM vendor. This occurred due to a vishing attack, where the attacker faked the identity of an employee when ringing the MGM help desk. After gaining access to Okta, the attacker could then go on to effect wider areas of MGM's network.

$100 Million

Estimated cost
of the MGM breach

More recently, password management company, 1Password, were also impacted due to a security incident relating to an Okta breach. Fortunately, 1Password have claimed no user data or sensitive information was compromised.

Nevertheless, these examples both highlight that IAMs need to have stringent cyber security measures in place. While IAMs are designed to be secure, the mantra of cyber security still holds true; nothing is 100% unhackable.

The following pages outline the best practices to ensure an organisation's IAM remains secure.

Best Practices for IAM

Effective IAM depends on people, processes, and technology across an organisation. Here are some of the best practices to build a robust IAM program:

- Document IAM policies and procedures clearly
- Classify data by sensitivity and assign access levels accordingly
- Integrate IAM processes with HR systems for user lifecycle management
- Use role-based access control (RBAC) to restrict privileges
- Implement multifactor authentication (MFA) for additional user verification
- Review user entitlements and access rights regularly
- Maintain well-defined incident response plans for IAM breaches
- Monitor user activities for security incidents and policy violations

Building comprehensive IAM standards with appropriate controls takes time but pays dividends in improved security and compliance. With thoughtful planning and disciplined execution, organisations can strike the right balance between ensuring security, while maintaining usability.

TELESOFT

How Telesoft Can Help

Full Network Visibility in Real-Time

Telesoft provide high-rate network monitoring tools that can be designed specifically for your organisation's needs. TDAC Enterprise is a virtualised software solution that provides complete network visibility for analysts.

TDAC Enterprise ingests raw network traffic and enriches it with the latest threat intelligence, allowing organisations to identify threats within their network, including across IAM tools.

24/7 Managed Security Service

Lack the resources to coninuously monitor your network?

Our Managed Detection and Response (MDR) service provides a comprehensive cyber security solution, offering full network visibility and 24/7 proactive monitoring from our UK-based Security Operations Centre.

Our expert team of cyber analysts will monitor your network environment, including cloud applications such as Okta and other IAM tools. This means our team would be able to rapidly alert you to any suspicious activity detected, including unauthorised and suspicious logins to your organisation's IAM application.

TELESOFT

Conclusion

Identity access management platforms offer significant benefits in terms of centralising user authentication and enabling secure access controls. However, as with any centralised system, IAM also introduces risks if not properly secured. Recent breaches at MGM and 1Password highlight the need for robust security practices.

Organisations should implement a layered approach to secure their IAM platforms and integrations. Policies, access controls, activity monitoring, and incident response plans are all critical. Leveraging solutions such as Telesoft's 24/7 Managed Detection & Response service can also significantly reduce risk by enabling fast identification and response to any detected threats within an organisation's network.

Book a call for a demo of our cyber security solutions:

Email:
sales@telesoft-technologies.com

Website:
www.telesoft-technologies.com/contact-us

TELESOFT