Ironcore Resources

ZERO TRUST AWARENESS: IDENTITY

IDENTITY AND ZERO TRUST

Identity is a fundamental component of any security strategy, and it is especially critical in the context of Zero Trust. The Zero Trust security model is based on the principle of never trusting any user or device by default, whether inside or outside the network perimeter. In this model, every user, device, and application must be authenticated and authorized before gaining access to any network resource.

WHY IT'S IMPORTANT

OVER 80%

Over 80% of all attacks involve credential use or misuse in the network.

4 OUT OF 5

Four out of five breaches are caused by sources external from the victim organization.

$1 MILLION

Organizations that don't deploy Zero Trust experience an average cost increase of $1 million in the year following a breach.

COMPLIANCE:

Many regulations and standards require organizations to implement strong identity and access controls to protect sensitive data. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires organizations to implement strong authentication mechanisms to protect cardholder data.

SECURITY:

Zero Trust's identity-centric approach ensures that access controls can be granularly applied, enabling organizations to enforce least privilege principles. Limiting network access to only the users and devices that have been authorized and deemed necessary to access specific resources minimizes attack surface.

VISIBILITY:

By using identity to authenticate users and devices, organizations can gain visibility and control over their IT environments by tracking who is accessing what resources and monitoring their activities. This visibility enables organizations to detect and respond to security incidents more quickly, reducing the impact of potential data breaches.

IRONCORE
STRONG · TRUSTED · SECURE

www.ironcore-inc.com
zerotrust@ironcore-inc.com / 608-779-9400

IDENTITY EXAMPLES

In the Zero Trust security model, identity is used to establish trust in users and devices before granting them access to resources. This means that all users and devices must be identified and authenticated before being granted access to any network resource.

TRADITIONAL METHODS

Username and password
Multi-Factor Authentication
Biometrics
Limited risk assessment

OPTIMAL METHODS

Use of Identity and Access Management platforms
Review of security standard satisfaction
Real time machine learning analysis
Continuous validation

CONSIDERATIONS

IDENTITY AND ACCESS MANAGEMENT

Minimizing the number of Identity and Access Management (IAM) platforms is also important. Most modern applications and services can utilize various forms of Single Sign On (SSO) to authenticate and authorize against your chosen IAM platform, allowing you to manage and monitor authentication and access from a single platform. Examples of IAM platforms are Microsoft Active Directory, OKTA and Microsoft Azure Active Directory.

MANAGING IDENTITY OVER TIME

It is important to note that managing identity is not a one-time process, but rather an ongoing effort that requires regular review and updates. Changes to compliance requirements, adjustments to access privileges, and updates to organizational security standards can all impact identity policies. Organizations that implement a Zero Trust security model with strong identity and access controls can significantly improve their security posture and protect against data breaches.

SUBSCRIBE TO OUR BLOG

Scan the QR Code or visit www.ironcore-inc.com/blog to follow more educational series like this.