How to A.C.E. Your Firm’s Security

Authentication, Communication, Encryption

Information security is fast moving and affects many parts of an organization. The speed of change that makes information security fun can also make it difficult to manage. Cloud services add to the complexity by dramatically changing the security landscape and breaking down the traditional borders protecting our information. As things change in your environment, what should you be paying attention to around security? The Adaptive Solutions A.C.E. security model outlines three components of security that can help you manage change within on-premise or cloud environments.

Authentication

It’s important to know who has access to what information in your firm. User authentication, the process that allows a device or system to verify the identity of users, can impact how well your organization controls information.

The most secure framework for authentication is a centralized system. Active Directory and LDAP configuration can be used for VPN, System, and device authentication with on-premise systems. An ID provider of your choice, such as Azure AD, ADFS, Ping, Workspace One, etc., can be used for a cloud-based single sign-on (SSO) authentication.

There are several advantages to centrally managing user accounts:

- Users have single username and password for all services, reducing the number of shared accounts;
- Easier enforcement of least access permissions;
- Improved logging of user activity and change management;
- Simpler administration of permissions across the network;
- Enforcement of multi-factor authentication (MFA) and security policies such as password complexity requirements, across the entire infrastructure.

Communication

Understanding how data is secured in transit is essential to protecting the firm’s information and client documents. Many systems have both secure and insecure options that define how they can communicate. Be sure your project and systems use the secure option.

At the heart of secure communication are certificates. Certificates allow two devices to trust each other using a public and private key pair. There are different types of certificates, including self-signed, internal, and public. Understand how certificates are used and protected in your organization.

Encryption

People often wonder why data would need to be encrypted, when it is in a locked data center, and there is a guard. It’s common for people to question the value of encrypting data at rest, but it is worthwhile.
Information security is a game of defense in depth. Encryption at rest is a cost-effective last line of defense for your data whenever other controls break down. This control is particularly valuable with mobile devices that are easily stolen or lost, which may contain large amounts of data.

For cloud-based services, this control has additional value. Most cloud service providers encrypt your data at rest, but they often keep the private key. This allows them to produce the contents of your data for as long as they have a copy. If a firm brings their own private key to encrypt the data, they can revoke access to the data and prevent the provider from accessing it in the future for any reason.

So, remember the ACE acronym: Authentication, Communication, Encryption. Understanding and making the right choices in these three key areas will increase the effectiveness of your firm’s information security.