7 Deadly Sins

DREW Blandford-Williams
GRC
cybersecurity consulting services

CLOUD Security

Weak Credentials

Ignoring weak passwords and allowing easy-to-guess formats for user access can bring unwanted access! Data breaches invite a host of trouble, from lawsuits to fines—to loss of business!

Authentication Gaps

Cloud breaches often result from insufficient access control. Implementing multi-factor authentication, frequently re-setting API keys & deleting unused credentials. Can reduce the risk of a compromise because of credential harvesting.

Misconfigured APIs

Improperly configured Application Programming Interfaces (APIs), and user interfaces have led to a majority of the data breaches in cloud environments. Keep those APIs private and look to API frameworks that consider “Security” as a priority!

Bad Cloud Configurations

Default configuration options and login credentials are two key reasons why misconfigurations are among the most common “sins” in cloud security. Misconfigured database servers, for example (which often contain admin password information), can lead to massive data compromises.

External Data Sharing

“Collaboration” between links invites trouble—especially if there’s on governance in place to oversee how to use this important cloud capability. Data that is not properly secured, which may be accessed via a public network, can lead to extensive compromises (“ransomware!”).

Unpatched Systems

Although common across all system operating platforms, patch management continues to be a challenge, even in a cloud environment. Unpatched or outdated software, frameworks, or libraries result in open-door invitations for system compromises, stolen data, and loss of access.

Absent / Inefficient Back-ups

Many organizations moving to the cloud overlook the need for a comprehensive Back-up, Recovery and Disaster Planning strategy. Without a disaster recovery or continuity plan can result in data loss, extended downtime, or inability to restore services in the event of a disaster.

grcdrew.com