ptp Infinite Innovation

8 COMMON AWS SECURITY MISTAKES

AND HOW TO FIX THEM

BY

Gary Derheim

1 IMPROPER S3 PERMISSIONS

S3 buckets are private by default, but an administrator can choose to make them public. This can be problematic if a user uploads sensitive or personal content and it becomes available online—which is precisely why we recommend against this for general use cases.

The AWS console gives you the power to control who has access and for what purposes. Using the AWS console, the following grantees can be given access to a bucket:

- Authenticated users (anyone with an AWS account)
- Log delivery
- Everyone (anonymous access)

The permissions that these grantees can be given are:

- List
- Upload/Delete View
- Permissions Edit
- Permissions

Users can also generate custom bucket policies that provide greater flexibility than the AWS console.

Depending on the bucket and the objects it contains, granting any of these permissions may or may not be cause for concern. However, any bucket with permissions granted to “Everyone” should be immediately reviewed.

ptp Infinite Innovation

2 LACK OF ENCRYPTION

As the risks associated with cyber crimes and data breaches continue to rise, it is more important than ever for businesses to process and protect information. The best way they can do this? By using encryption!

We believe almost all traffic should be encrypted, but this is especially true for financial and healthcare data. The performance hit of encrypting and decrypting data is negligible, and it ensures trust among web users when submitting forms. This is referred to as "Encryption in Transit."

Additionally, data in storage arrays should be protected from prying eyes. This is referred to as "Encryption at Rest." Enterprises need to ensure that there are no weak links in the chain when it comes to securing sensitive data.

ptp Infinite Innovation

3 IAM USERS DIRECT PERMISSIONS

Identity and Access Management (IAM) enables AWS users to control access to their account by creating and managing AWS users and permissions. In addition to creating users, IAM allows for the creation of groups. Permissions can be granted to a group, and any user that belongs to that group is given those particular permissions.

This streamlines permissions management, as each user does not have their own unique set of permissions, and administrators can quickly tell which users are allowed which permissions by the group to which they belong. Any users that have their own unique permissions should have those permissions revoked and be added to a group instead.

ptp Infinite Innovation

4 ACCIDENTAL PUBLIC AMI'S

Amazon Machine Images (AMIs) contain all the information necessary to launch an Amazon Elastic Compute Cloud (EC2) instance. They act as a template that contains the software configuration (operating system, application server, and applications) that will be used with the launched instance. AWS users can create their own AMIs, utilize public AMIs, or purchase custom AMIs.

When a user creates an AMI, they are given the option to make the AMI public, share it with specific AWS accounts, or make it private. Public AMIs can be launched by all AWS accounts and are shared in the AMI catalog.

However, because AMIs often contain proprietary or sensitive data, it is recommended that they always be set to private. Any AMIs that are publicly accessible should be carefully reviewed.

ptp Infinite Innovation

5 IMPROPERLY CONFIGURED CLOUDTRAIL

Amazon CloudTrail provides AWS users with a complete history of all of the API calls made against their account. This includes calls made from the AWS Management Console, SDKs, command line tools, and other AWS services. CloudTrail creates log files of this data and deposits the log files into a designated S3 bucket. Included in log files is the source IP address of the calls and the date and time of the calls.

Administrators should have CloudTrail enabled within the AWS account so that they always know who and from where the AWS account is being accessed.

ptp Infinite Innovation

6 LOGGING ON ALL S3 BUCKETS

Logging must be manually enabled on any S3 bucket, as it is disabled by default. When enabled, an access log record will be created for all requests made against a bucket containing the request type, resource with which the request worked, and the date and time the request was processed.

As with CloudTrail, having logging enabled on all S3 buckets is important as it provides insight into the nature of the requests made against the buckets. This also allows administrators to determine whether a resource is receiving heavy traffic, which means that it may have been left public by accident.

ptp Infinite Innovation

7 IP ADDRESS RANGES IN VPC

A Virtual Private Cloud (VPC) functions like a VPN, enabling users to launch AWS resources in an isolated virtual network. Administrators can control who has access to the virtual private cloud by selecting IP address ranges, creating subnets, and configuring route tables and network gateways, depending on the level of security they need.

Because this is a customizable solution, cloud admins need to define the permissions in their virtual private cloud environment. Only specific IP ranges should be specified for the VPC and only needed ports should be exposed. Leaving the VPC open to all ports and all IP addresses is highly discouraged because it creates a large attack surface for a malicious user.

ptp Infinite Innovation

8 IMPROPER NACL TRAFFIC CONFIGURATION

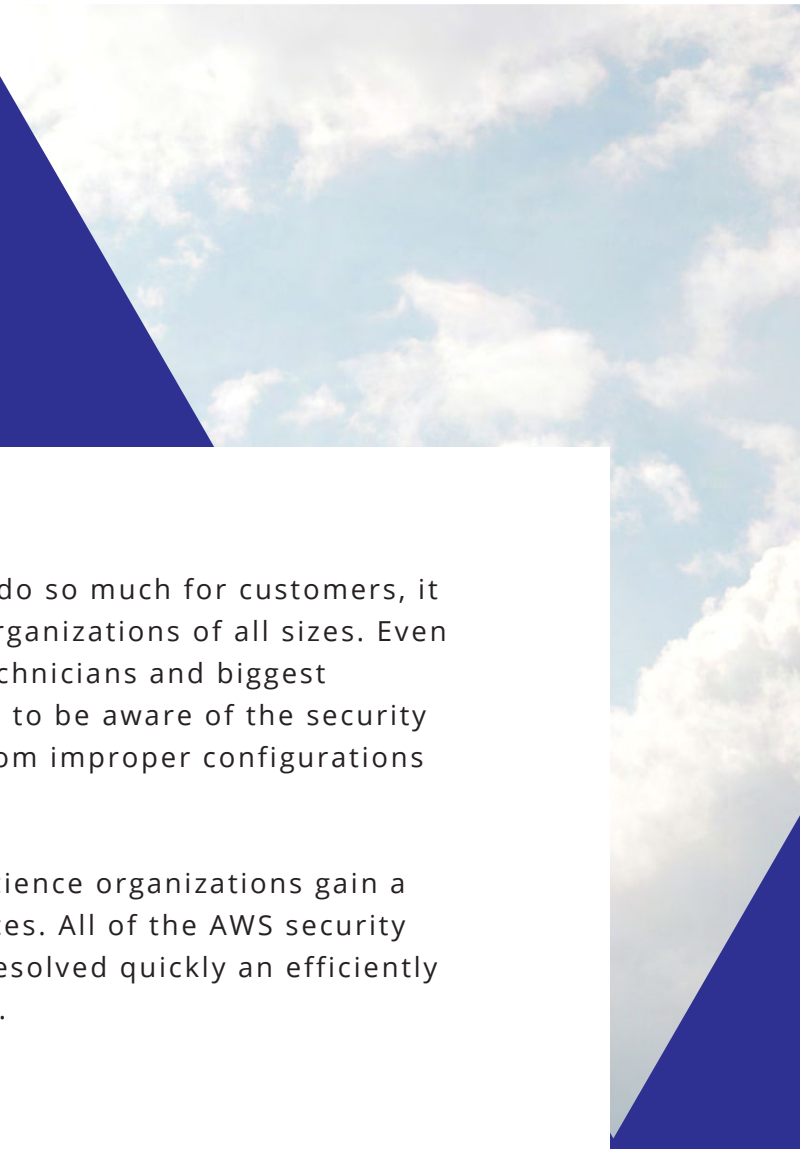
A network access control list (NACL) is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. Administrators can set up NACLs with rules similar to their security groups in order to add an additional layer of security to a VPC.

Rules within an NACL are evaluated based on a rule number set for the rule. AWS allows or denies packets depending on the first rule to match the request. The lowest or first-numbered rule to match takes priority and is used.

In a default VPC, it's common to see NACL rule #100, which allows all inbound ports and IP addresses. One best practice is to restrict traffic to only necessary ports and IP addresses. If administrators find an NACL open to all ports and IP addresses, they should remove the rule and create more restrictive rules to allow only the appropriate inbound traffic.

ptp Infinite Innovation

WHY ARE THESE AWS SECURITY ISSUES SO COMMON?



While AWS has the capability to do so much for customers, it is also a complex platform for organizations of all sizes. Even the most highly trained cloud technicians and biggest information security teams need to be aware of the security vulnerabilities that can result from improper configurations and permissions within AWS.

Fortunately, PTP can help Life Science organizations gain a foothold on security best practices. All of the AWS security issues described above can be resolved quickly an efficiently though PTP's CloudOps program.

ptp Infinite Innovation