Loss of Reputation/Value (version 1.0)

**Cloud Service Label: IaaS, PaaS, SaaS**

Description

Consumers of cloud services and especially IaaS resources have effectively accepted responsibility (liability?) of all such resources. In the public’s view there is little distinction between an organization’s effectiveness and its ability to manage its computing resources. If cloud resources under the purview of an organization are used for malicious or salacious purposes, the damage to intuitional reputation could be immense. HB Gary, a computer security company, suffered severe reputational and financial harm after an affiliate’s website was compromised. Capitol One suffered reputational and financial harm after a former AWS employee compromised thousands of Capitol One customer’s data inside AWS S3 buckets. AWS did not seem to suffer significantly, but Capitol One shares dropped almost 7% because of the incident.

In the cloud, S3 buckets that are controlled by an organization and misconfigured to allow writes can be accessed and used by any third party to store and distribute illicit material and have the organization foot the bill.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| GhostWriter | McAfee initiative discovered thousands of S3 buckets configured to allow anonymous, unauthenticated writes among some of the largest corporations in the world. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Audit | | Frequently check permissions on cloud storage to ensure proper permissions are set to deny open or unprivileged access to resources. Consider using automated resource checkers such as CloudSploit or Divvycloud. |
|  | *AWS* | To perform an audit via AWS it is suggested to review information such as account details (credentials, users, groups, roles, etc), mobile applications, EC2 configurations, policies, and account activity. How to audit these different factors can be found in detail at: **https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html.** |
|  | *Azure* | To perform an audit via Azure an administrator can review the audit logs that are recorded under Azure’s monitoring for active directory. The audit logs allow for filtering, as well as looking at users, groups, and enterprise specific information. Full details on how to access this information can be found at: **https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs.** |
|  | *GCP* | To perform an audit via GCP the logs can be reviewed. GCP breaks this down into three categories; admin activity, data access, and system events. The audit logs can be viewed a few different ways- the console, API, or gcloud. Full details on how to view these logs, how to export, and for how to configure the retention period can be found here: **https://cloud.google.com/logging/docs/audit.** |
| Encrypt Sensitive Information | | Encrypt data stored at rest in cloud storage. Managed encryption keys can be rotated by most providers. At a minimum, ensure an incident response plan to storage breach includes rotating the keys and test for impact on client applications. |
|  | AWS | To encrypt data at rest in an AWS environment first start by configuring the IAM roles and permissions. A policy will need to be created to specify that the data is to be encrypted and then the policy is attached to the instance. Full details on how to accomplish this can be found at: **https://aws.amazon.com/blogs/security/how-to-protect-data-at-rest-with-amazon-ec2-instance-store-encryption/**. |
|  | Azure | To encrypt data at rest in an Azure environment it can be done differently depending on the cloud service the customer is utilizing. For SaaS customers this can be enabled or available on each specific service. For PaaS customers there are specific storage and application platforms that can be used. In terms of IaaS customers this can be broken down to a couple different aspects. Encrypted storage can be enabled the same as PaaS services, utilizing other Azure services. Encrypted compute allows for all managed disks, snapshots, and images to be encrypted utilizing a service managed key. The keys are stored in the Azure key vault. Full details on how to accomplish this can be found at: **https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest.** |
| Filter Network Traffic | | Cloud service providers support IP-based restrictions when accessing cloud resources. Consider using IP whitelisting along with user account management to ensure that data access is restricted not only to valid users but only from expected IP ranges to mitigate the use of stolen credentials to access data. In Azure storage resources can be tied exclusively to a particular virtual network reducing the chances that it can be accessed externally or from other cloud assets. |
|  | *AWS* | An AWS environment can be configured with network ACLs (access control lists) to allow or deny inbound and outbound traffic. This can be accomplished by accessing Amazon VPC and navigating to either inbound or outbound rules depending on the rule the user wishes to add and they can be added, removed, or edited from that panel. Full details about ACLs and how to add rules in AWS can be found here: **https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html.** |
|  | *Azure* | In Azure storage resources can be tied exclusively to a particular virtual network reducing the chances that it can be accessed externally or from other cloud assets. This can be done multiple ways including the Azure Portal, Azure PowerShell, and Azure CLI (Command Line Interface). Depending on the method used to implement this the procedure can vary, but will include the need to create a security group, create a network security group, associate that network security group with a specific subnet and then create security rules that are associated to the inbound and outbound rules for that subnet. Full details on how to configure this utilizing the various methods can be found below:  Azure Portal: **https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic**  Azure PowerShell: **https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic-powershell**  Azure CLI: **https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic-cli** |
| Multi-Factor Authentication | | Use multi-factor authentication for user and privileged accounts. Do not manage Cloud portals from machines that perform user email and web browsing tasks. All users should be required to utilize two factor authentication. |
|  | *AWS* | This can be enforced by first creating a policy that would prohibit actions except those that allow a user to change their password or manage 2FA, then attaching a policy to a group that includes all user accounts where they can be allowed all access if they sign in with 2FA. Once these actions are completed it should be tested to verify the access is given correctly. To see full details on how to complete this view AWS documentation at: **https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\_users-self-manage-mfa-and-creds.html.** |
|  | *Azure* | This can be done by creating a MFA registration policy. It can than be assigned to all users (with the ability to exclude some if need be, but is not recommended). Make sure once the policy is created and added to users that it is then being enforced, once enforced it should be tested for verification. To see full details on how to complete this view Azure documentation at: **https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy.** |
|  | *GCP* | This can be done by first enabling it on the current account being used by admin to assign the roles, then enable two factor on an instance by instance or project by project basis, then assigning the requirements based on IAM roles and applying it to all users. To see full details on how to complete this view Azure documentation at: **https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication.** |
| Restrict File and Directory Permissions | | Users should have limited access to files and directories depending on their need for access. The file and directory permissions should be restricted on the basis of least privilege. |
|  | *AWS* | To manage the files and directory permissions in AWS, IAM policies can be used. This can be done by utilizing group policies and policy variables. The policy would be created specifying the folder, then the permissions attached to that folder (whether the user has access to list out the objects within the directory, if they have read permissions, if they have write permissions, etc.), lastly the group that it applies to would be specified. The users can that be added and removed from that group as needed. Full details on how this can be done is explained here: **https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/.** |
|  | *Azure* | To manage the files and directory permissions in an Azure environment basic and advanced system defined controls. This will be dependent on the type of system being used (Windows, Linux, etc). The permissions will be set individually or by group using the system commands or controls needed.. Full details on how this can be done is explained here: **https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-configure-permissions.** |

Detection

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Create Log Metric Filters and Alarms for AWS | To create a metric filter and alarm:   1. Create a metric filter that checks for IAM policy changes and the *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter and SNS topic created in steps 1 and 2 respectively |
| Monitor Activity in AWS Account | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3. |
| Monitor for Suspicious Activity in Azure | Azure AD can generate anomaly reports than can be run on a daily basis. Azure AD Identity Protection show current risks in its dashboard and provides daily email summary notifications. Policies can also be configured to alert to specific issues. |
| Create Log Metric Filters and Alarms for CloudTrail | To create a metric filter and alarm:   1. Create a filter that checks for CloudTrail changes and the specific *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic that the alarm will notify 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter from step 1 and SNS topic in step 2 |
| Create Activity Log Alerts in Azure | To create log activity alerts for deletion in the Azure Console:   1. Navigate to *Monitor’ / ‘Alerts* 2. Select *Manage alert rules* 3. Click on the Alert *Name* where Condition contains *operationName equals Microsoft.Network/networkSecurityGroups/securityRules/delete* 4. Hover a mouse over *Condition* to ensure it is set to *Whenever the Administrative Activity Log “Delete Security Rule (networkSecurityGroups/securityRules)” has “any” level with “any” status and event is initiated by “any*” |
| Create, View, and Manage Activity Alerts in Azure Monitor | To create a log alert in the Azure portal:   1. Select **Monitor -> Alerts** 2. Select **New alert rule** of the **Alerts** window 3. Provide information in **Define alert condition** 4. Provide details in **Define alert details** 5. Specify action group for new alert rule under **Action group**, or create a new action group with + **New group** 6. Select **Yes** for the **Enable rule upon creation** option 7. Select **Create alert rule**   To view and manage alerts:   1. Select **Monitor -> Alerts -> Manage alert rules** 2. Select the rule you want to modify and double-click to edit the rule options 3. Click **Save** |
| Azure Resource Manager Templates | Azure Resource Manager templates in the format of JSON files that can be used to configure metric alerts in Azure Monitor. These templates can be used for simple static and dynamic threshold metric alerts, availability tests, and monitoring multiple resources. |
| Enable S3 Bucket Logging | To enable CloudTrail S3 bucket logging:   1. Navigate to CloudTrail console at Go to the Amazon CloudTrail console 2. Click Trails in the API activity history pane on the left 3. Sign into AWS Management Console and open the S3 console Sign in to the AWS Management Console and open the S3 console 4. Click on a bucket under *All Buckets* 5. Click on *Properties* 6. Under *Bucket:\_<bucket\_name>\_* click *Logging* 7. Ensure *Enabled* is checked |
| Enable Azure Storage Logging | This is used to track how requests made to Azure Storage were authorized. Enabling logs provides visibility into whether a request was anonymous, made with an OAuth2.0 token, a shared key, or shared access signature (SAS). Full Azure Storage analytics logging details can be found at [**https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?tabs=dotnet**](https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?tabs=dotnet)**.** |
| Enable CloudTrail across all regions in AWS | To enable CloudTrail across all regions:   1. Sign into the AWS Management Console and open the CloudTrail console 2. Click on *Trails* 3. Set necessary Trails to All option in the I column 4. Click on a trail via the link *Name* column 5. Set *Logging* to *ON* 6. Set *Apply trail to all regions* to *Yes* |
| Configure log profile to capture activity logs for all regions in Azure | To set up activity logs for all regions:   1. Navigate to Azure console 2. Go to *Activity log* 3. Select *Export* 4. Select *Subscription* 5. Check *Select all* in *Regions* 6. Select *Save* |
| Monitoring for Regional Activity | Tools like Splunk or even CloudSploit have the ability to alert based on region and ingest CloudTrail logs. In CloudSploit, a plugin called EC2 Max Count can be configured to alert after a certain threshold of EC2 instances is met. Real-Time Events service is another feature of CloudSploit that allows alerts for activity in unused regions. |

References

1. https://www.skyhighnetworks.com/cloud-security-blog/skyhigh-discovers-ghostwriter-a-pervasive-aws-s3-man-in-the-middle-exposure - Accessed Feb 12, 2020
2. https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says -Accessed March 2, 2020