Trusted Relationship (version 1.0)

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

Description

Adversaries may breach or otherwise leverage organizations and systems that have access to targeted cloud assets. Access through a trusted relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network. These connections include on-premise assets and logically separate cloud assets that afford special access to a customer’s cloud resources. Organizations often grant elevated access to on-premise systems and third party external providers including SaaS providers in order to allow them to manage cloud assets or share information. Some examples of these relationships include IT services contractors, managed security providers, and infrastructure contractors. Azure permits the creation of guest accounts to allow external organizations to access certain resources. These accounts probably will not be automatically culled from the system if the user leaves the guest organization as would likely happen in the host organization. This could result in accesses being permitted for unauthorized persons.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Co-Residence Identification and Information Leakage | As pointed out in a research paper written by the University of California San Diego and the Massachusetts Institute of Technology, co-residence is the process of identifying cloud instances that share the same underlying physical infrastructure, despite being separated virtually. Cloud users trust the cloud provider to ensure separation between different customers, however it is possible for a motivated customer to theoretically ensure co-residence with another customer on the same physical cloud host. Once virtual machine co-residence has been established, it might be possible to infer keys or other access credentials from co-resident machines leveraging their shared cache. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Audit for unusual activities that might be related to this activity | | Guest accounts should be audited more frequently to ensure external relationships are still valid. |
|  | 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.** |
| Network Segmentation | | Network segmentation can be used to isolate IaaS components that do not require broad network access. |
| User Account Control | | Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary. AWS and Azure can assign roles to its entities, which allows for strong IAM policies for various services like serverless functions, containers, or workloads. |
| Making Trust Determinations | | Trust determinations in Azure AD can be made through Hybrid Identity, Azure AD Connect, password hash synchronization, pass-through authentication, federation, and single sign-on. |
| Least Privilege | | All access given to users in the cloud environment should be assigned by the necessary privileges needed for team members to complete their job responsibilities. |
|  | *AWS* | To implement least privilege in an AWS environment IAM policies will be used. This gives the ability to allow users to perform list, read, write, permissions management, or tagging actions. AWS suggests utilizing *last accessed information* and A*WS CloudTrail event history* to get a better understanding of privileges that might be needed or reduced based on a specific role. Full details can be found at **https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege.** |
|  | *Azure* | To implement least privilege in an Azure environment Azure Active Directory roles will be used. Azure outlines different tasks and the least privileged role that are suggested to be associated with the task. Those details can be found at: **https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-delegate-by-task.** To learn how to assign specific roles it can be done via the Azure Active Directory Portal. Instructions on how to assign roles can be found here: **https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-manage-roles-portal.** |
|  | *GCP* | To implement least privilege in GCP it is recommended to use predefined roles (which allow for granular access permissions) instead of primitive roles (roles/owner, roles/editor, and roles/viewer). Full details on the difference between types of roles can be found here: **https://cloud.google.com/iam/docs/understanding-roles.** To assign these roles IAM service accounts are used and complete details can be found at: **https://cloud.google.com/iam/docs/using-iam-securely#least\_privilege.** |

Detection

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Monitoring | | Establish monitoring for activity conducted by second and third party providers and other trusted entities that may be leveraged as a means to gain access to the network. Depending on the type of relationship, an adversary may have access to significant amounts of information about the target before conducting an operation, especially if the trusted relationship is based on IT services. Adversaries may be able to act quickly towards an objective, so proper monitoring for behavior related to Credential Access, Lateral Movement, and Collection will be important to detect the intrusion. |
|  | AWS | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3.  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 |
|  | 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.  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** |
| CASB (Cloud Access Security Broker) | | Consider employing a CASB to monitor access between SaaS accounts and AWS/Azure resources. |

References

1. <https://sonraisecurity.com/education/aws-azure-google-cloud-security-iam/>. Accessed July 27, 2020.
2. <https://devblogs.microsoft.com/azuregov/implementing-zero-trust-with-microsoft-azure-identity-and-access-management-1-of-6/>. Accessed July 27, 2020.
3. https://cseweb.ucsd.edu/~savage/papers/CCS09.pdf. Accessed July 2, 2020.
4. Wait a minute! A fast, Cross-VM attack on AES Gorka Irazoqui, Mehmet Sinan Inci, Thomas Eisenbarth, and Berk Sunar Worcester Polytechnic Institute, Worcester, MA, USA – Accessed August 6,2020