TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO ĐỒ ÁN CLOUD SECURITY

Bộ môn: Seminar Công nghệ tri thức

Giảng viên: Ngô Minh Nhựt

Lê Long Quốc

Nhóm thực hiện:

20127318: Phan Trí Tài

Hồ Chí Minh, ngày 17 tháng 12 năm 2023

Table of Contents

Giới thiệu về điện toán đám mây

Điện toán đám mây là mô hình điện toán sử dụng công nghệ máy tính và phát triển dựa vào mạng Internet. Điện toán đám mây là mô hình cung cấp tài nguyên máy tính cho người dùng tùy theo mục đích sử dụng thông qua kết nối Internet. Nguồn tài nguyên này bao gồm rất nhiều thứ liên quan đến điện toán và máy tính, ví dụ như: phần mềm, dịch vụ, phần cứng,… và sẽ nằm tại các máy chủ ảo (đám mây) trên mạng. Người dùng có thể truy cập vào bất cứ tài nguyên nào trên đám mây. Vào bất kỳ thời điểm nào và ở bất kỳ đâu, chỉ cần kết nối với hệ thống internet.

Những thách thức bảo mật đám mây

Securing third-party software and insecure APIs: Phần mềm dễ bị tổn thương của bên thứ ba và các API không an toàn có thể mở rộng phạm vi tấn công của doanh nghiệp do vô tình cung cấp quyền truy cập quá mức. Nghiên cứu của chúng tôi cho thấy chỉ có 18% doanh nghiệp thiết lập ranh giới cấp phép tối ưu cho các ứng dụng của bên thứ ba. Phần còn lại cung cấp các đặc quyền quá mức và làm lộ dữ liệu nhạy cảm.

Lack of visibility: Khả năng hiển thị không đầy đủ trong môi trường đám mây có thể dẫn đến khó khăn trong việc giám sát và xác định các mối đe dọa bảo mật tiềm ẩn. Việc thiết lập các cơ chế hiển thị toàn diện là điều cần thiết để bảo mật hiệu quả.

Lack of cloud security professionals: Việc thiếu các chuyên gia lành nghề có chuyên môn về bảo mật đám mây đặt ra một thách thức. Các tổ chức cần đầu tư vào đào tạo hoặc thuê các chuyên gia có kiến thức về bảo mật môi trường đám mây.

Cloud data governance: Các thách thức về quản trị dữ liệu trên đám mây bao gồm:

- Khả năng hiển thị trên các nhóm công khai AWS, GCP và Azure, khối lượng dữ liệu và cơ sở dữ liệu được quản lý
- Phát hiện phơi nhiễm dữ liệu
- Hiểu luồng dữ liệu và dòng dữ liệu
- Triển khai chính sách
- Tuân thủ

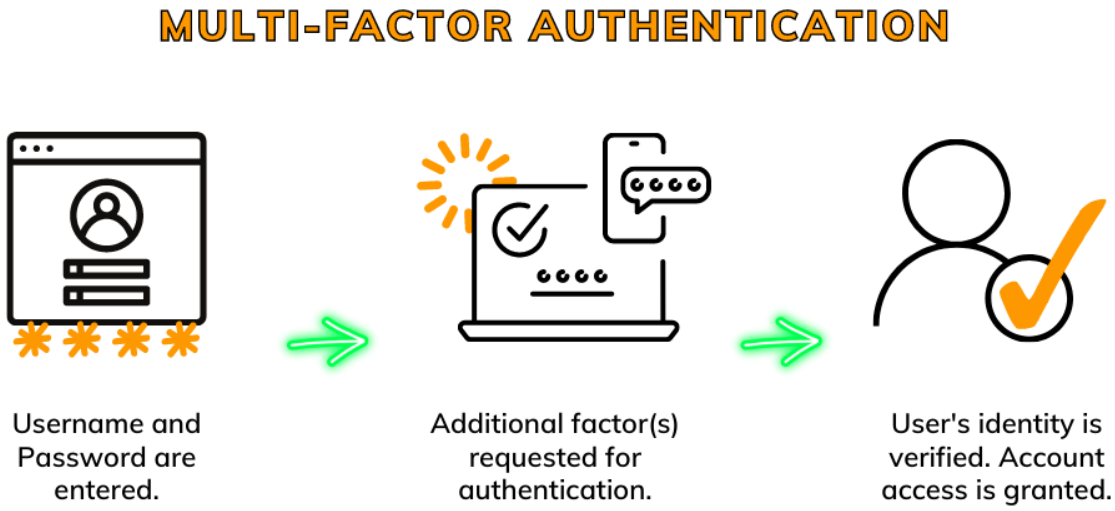
Shadow IT: Việc sử dụng các dịch vụ đám mây trái phép hoặc không được giám sát trong một tổ chức (Shadow IT) có thể gây ra rủi ro bảo mật. Việc triển khai các chính sách kiểm soát, giám sát việc sử dụng dịch vụ đám mây là điều cần thiết.

Managing a rapidly evolving attack surface: Bề mặt tấn công trong đám mây rất năng động và có thể thay đổi nhanh chóng. Thường xuyên cập nhật các biện pháp bảo mật, tiến hành đánh giá rủi ro và cập nhật thông tin về các mối đe dọa mới nổi là rất quan trọng.

Multi-cloud security: Những lo ngại về bảo mật có thể nảy sinh khi một tổ chức sử dụng nhiều nhà cung cấp dịch vụ đám mây. Đảm bảo các chính sách bảo mật và kiểm soát nhất quán trên các môi trường đám mây khác nhau là một thách thức đòi hỏi phải có sự quản lý cẩn thận.

Kỹ thuật bảo mật đám mây

Multi-Factor Authentication (MFA)



Firewalls and Network Security

Authentication software chịu trách nhiệm chính trong việc đảm bảo rằng một cá nhân hoặc máy tính được phép truy cập tài nguyên trên đám mây.

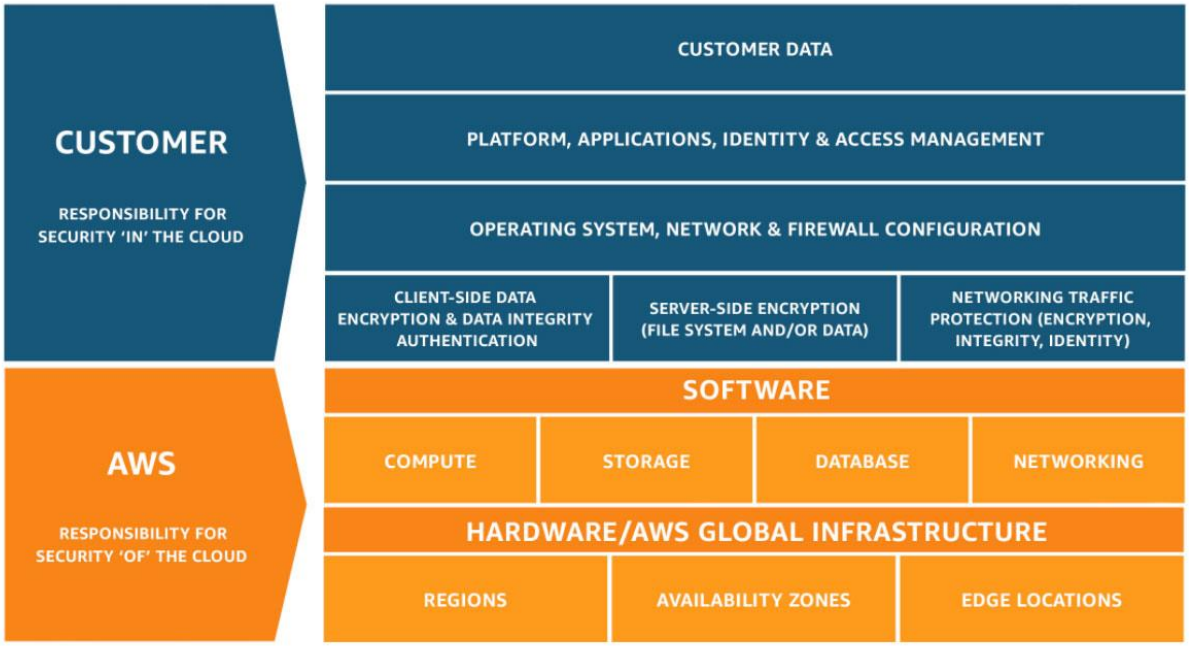
Encryption đề cập đến quá trình mã hóa dữ liệu thành định dạng không thể nhận dạng được. Do đó, nếu hacker truy cập vào dữ liệu của bạn, bạn sẽ cần một khóa mã hóa để giải mã dữ liệu của mình.

Data integrity đảm bảo rằng dữ liệu thể hiện những gì chúng ta mong đợi.

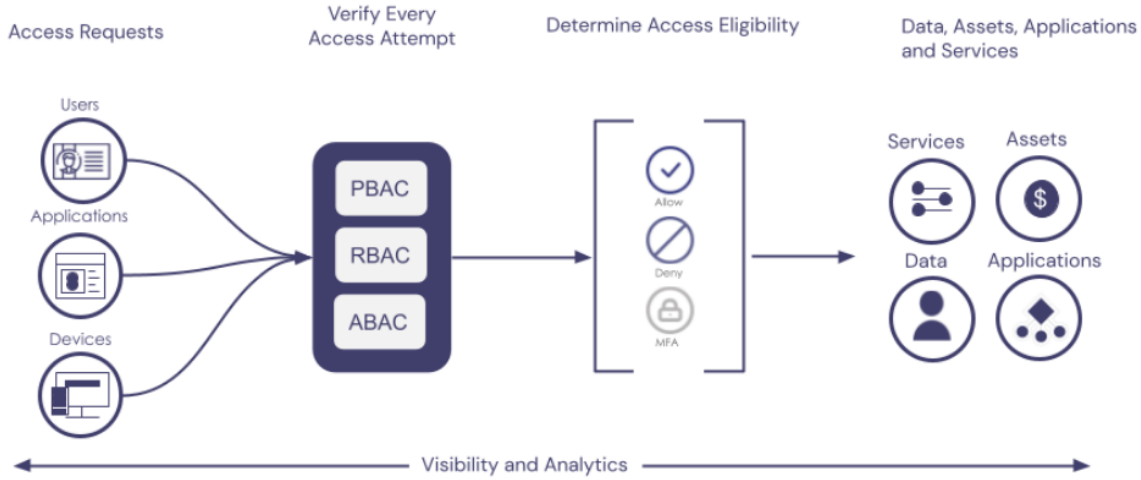
Có nhiều kiểu tấn công vào đám mây. Để ngăn chặn một số cuộc tấn công này, bạn có thể vô hiệu hóa một số cổng trên đám mây, cài đặt các biện pháp chống vi-rút mới nhất hoặc sử dụng tường lửa để ngăn chặn các cuộc tấn công.

Kiến trúc bảo mật đám mây

Shared Responsibility Model là cách mà Nhà cung cấp dịch vụ đám mây (CSP) và khách hàng chia sẻ trách nhiệm về bảo mật khi sử dụng dịch vụ đám mây.



Zero Trust Architecture là một mô hình bảo mật không yêu cầu sự tin cậy vào bất kỳ nguồn nào, ngay cả những nguồn nằm trong mạng nội bộ.



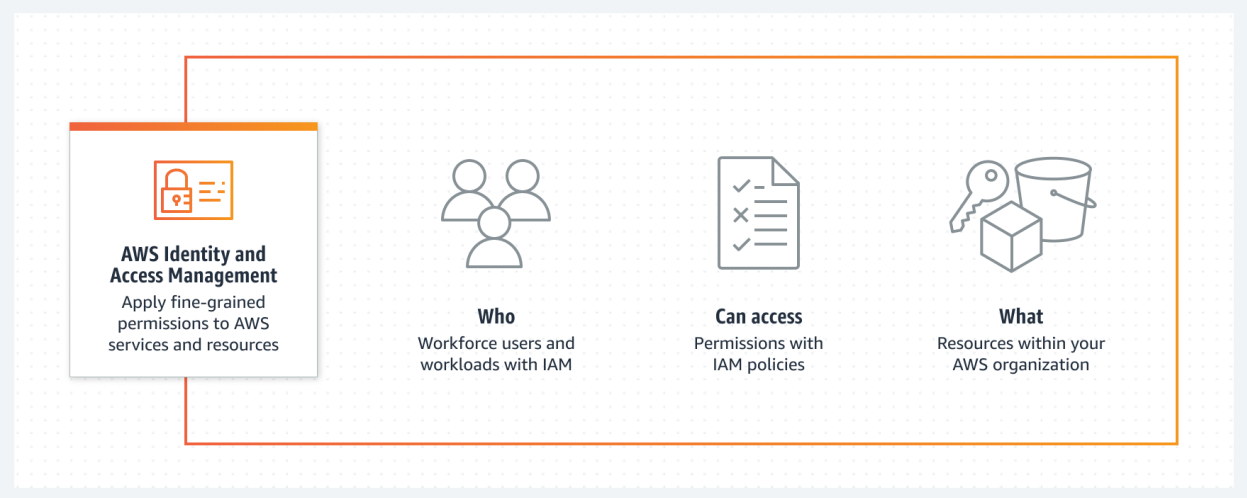
Microservices Security tập trung vào việc bảo vệ các ứng dụng và dịch vụ được xây dựng bằng kiến trúc Microservices. Nó thường bao gồm các biện pháp như xác thực, ủy quyền, mã hóa và quản lý khóa để đảm bảo an ninh trong môi trường phức tạp và phân tán của các dịch vụ độc lập.

Container Security liên quan đến việc đảm bảo sự an toàn và cách ly của các container, chẳng hạn như các container Docker. Nó bao gồm các biện pháp kiểm soát quyền truy cập, giám sát và bảo vệ khỏi các rủi ro bảo mật như chạy mã

độc hoặc can thiệp vào vùng chứa. Các biện pháp như quản lý hình ảnh an toàn, hạn chế đặc quyền của vùng chứa và quản lý khóa là những thành phần thiết yếu của bảo mật vùng chứa.

5 thành phần chính của kiến trúc bảo mật đám mây

Identity and Access Management (IAM)



Network Security: liên quan đến việc quản lý ai có thể truy cập tài nguyên đám mây và những hành động họ có thể thực hiện. Hệ thống IAM có thể thực thi các chính sách bảo mật, quản lý danh tính người dùng và cung cấp các bản kiểm tra cùng với các chức năng khác.

Data Security: Trong môi trường đám mây, an ninh mạng càng trở nên quan trọng hơn vì dữ liệu thường di chuyển qua internet để đến đám mây. Do đó, các tổ chức nên ưu tiên thực hiện các biện pháp an ninh mạng mạnh mẽ để bảo vệ dữ liệu của mình trong quá trình truyền tải.

Endpoint Security: Các biện pháp bảo mật điểm cuối bao gồm phần mềm chống vi-rút, tường lửa và các giải pháp quản lý thiết bị có thể thực thi các chính sách bảo mật trên thiết bị của người dùng. Hơn nữa, bảo mật điểm cuối cũng có thể bao gồm các biện pháp như đào tạo và nâng cao nhận thức cho người dùng, giúp người dùng nhận biết và tránh các mối đe dọa bảo mật tiềm ẩn.

Application Security: là một phần quan trọng khác của kiến trúc bảo mật đám mây. Nó liên quan đến việc bảo mật các ứng dụng chạy trên đám mây trước

các mối đe dọa bảo mật khác nhau, chẳng hạn như tấn công tiêm nhiễm, tập lệnh chéo trang (XSS) và Giả mạo yêu cầu chéo trang (CSRF).

Tiêu chuẩn bảo mật đám mây

- ISO 27017
- ISO 27018
- Cloud Security Alliance (CSA) STAR Program
- SOC 2 Type II
- NIST 800-53
- PCI DSS
- ….

Đồ án

Tạo một VPC (Mạng Riêng Ảo) với một subnet công cộng và hai subnet riêng tư có nghĩa là thiết lập một môi trường mạng ảo trong môi trường đám mây với các cấu hình cụ thể về khả năng tiếp cận mạng. Dưới đây là phân tích các thành phần chính và vai trò của chúng:

1. VPC (Mạng Riêng Ảo):

- VPC là một phần cách ly logic của đám mây, nơi bạn có thể triển khai và chạy các nguồn tài nguyên của mình. Nó cung cấp quyền kiểm soát đối với môi trường mạng ảo, bao gồm cả dải địa chỉ IP, các subnet và bảng định tuyến.

2. Subnet Công Cộng:

- Subnet công cộng là một phần của VPC có đường đi trực tiếp đến internet. Các nguồn tài nguyên triển khai trong subnet công cộng có thể có địa chỉ IP công cộng và có thể truy cập trực tiếp từ internet. Ví dụ về các nguồn tài nguyên thường đặt trong subnet công cộng là máy chủ web hoặc bộ cân bằng tải.

3. Subnet Riêng Tư (Hai subnet trong trường hợp này):

- Subnet riêng tư là các phần của VPC không có đường đi trực tiếp đến internet. Các nguồn tài nguyên trong các subnet riêng tư thường có địa chỉ IP riêng tư và không thể truy cập trực tiếp từ internet. Các subnet này thích hợp để triển khai các máy chủ backend, cơ sở dữ liệu hoặc các thành phần nội bộ không cần tiếp cận công cộng.

Bước để Tạo VPC với Một Subnet Công Cộng và Hai Subnet Riêng Tư

1. **Tạo VPC:**

- Xác định dải địa chỉ IP (CIDR block) cho VPC.

- Chọn số lượng khu vực khả dụng bạn muốn sử dụng.

2. **Tạo Subnet Công Cộng:**

- Xác định một subnet trong VPC và liên kết nó với một khu vực khả dụng cụ thể.

- Đảm bảo bảng định tuyến của subnet bao gồm một đường đi đến internet (thông qua Cổng Internet).

3. **Tạo Subnet Riêng Tư:**

- Xác định hai subnet bổ sung trong VPC, mỗi subnet liên kết với một khu vực khả dụng khác nhau.

- Các subnet này không nên có đường đi đến internet trong bảng định tuyến của chúng.

4. **Cổng Internet:**

- Tạo một Cổng Internet và gắn nó vào VPC.

- Liên kết Cổng Internet với subnet công cộng để cho phép các nguồn tài nguyên trong subnet đó giao tiếp với internet.

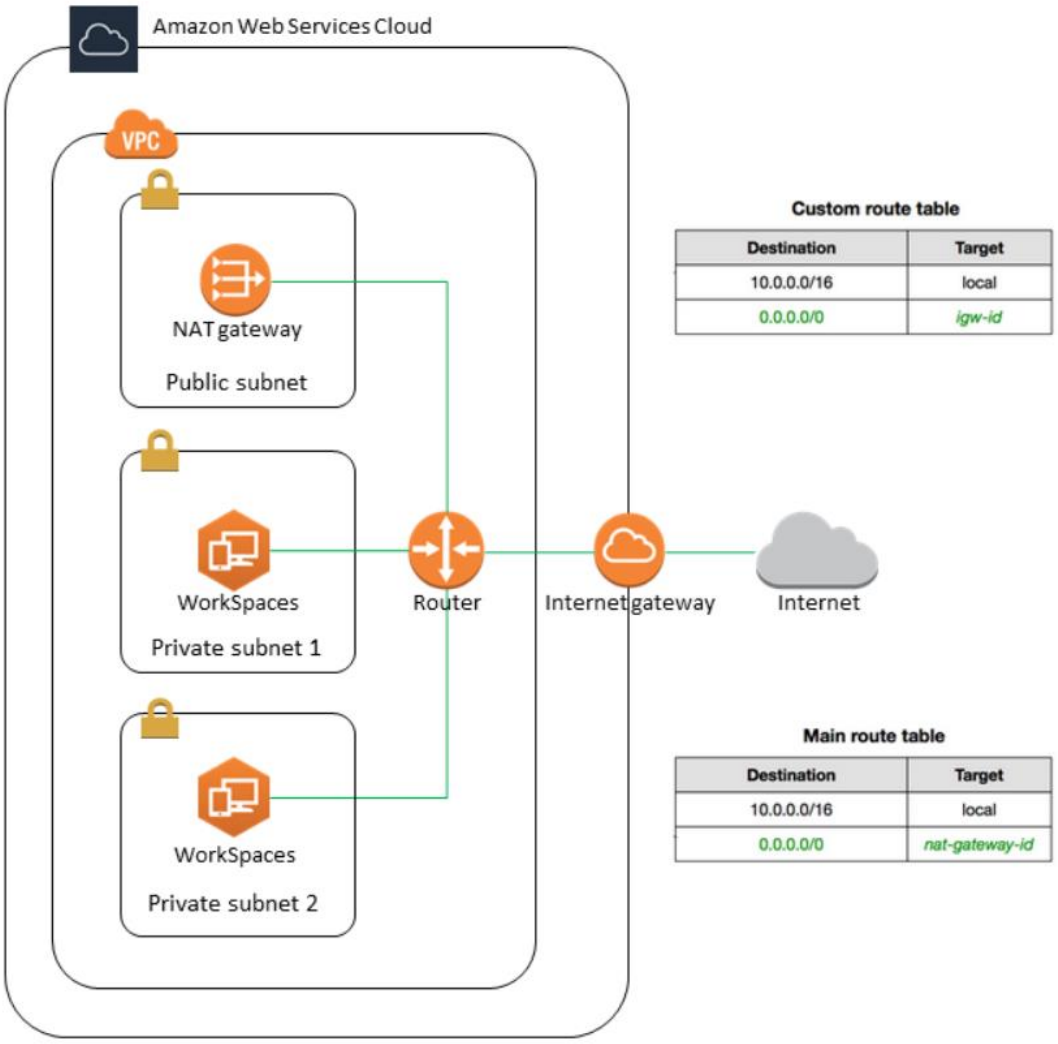
5. Bảng Định Tuyến:

- Tạo các bảng định tuyến riêng biệt cho subnet công cộng và từng subnet riêng tư.

- Liên kết subnet công cộng với bảng định tuyến có đường đi đến Cổng Internet.

- Liên kết từng subnet riêng tư với bảng định tuyến không có đường đi đến internet.

Bằng cách thực hiện các bước này, bạn sẽ thiết lập một VPC với một subnet công cộng cho các nguồn tài nguyên có thể truy cập internet và hai subnet riêng tư để tăng cường an ninh bằng cách cô lập các thành phần nhạy cảm.



Tài liệu

https://en.wikipedia.org/wiki/Cloud_computing_security

https://aws.amazon.com/vi/what-is-cloud-computing/

https://www.wiz.io/academy/cloud-security-challenges

https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-architecture/

https://www.aquasec.com/cloud-native-academy/cspm/cloud-computing-security-architecture/

https://aws.amazon.com/vi/compliance/shared-responsibility-model/

https://www.crowdstrike.com/cybersecurity-101/cloud-security/shared-responsibility-model/

https://www.skyflow.com/post/what-is-zero-trust

https://www.pingsafe.com/blog/cloud-security-standards/

https://sprinto.com/blog/cloud-compliance-guide/

https://ermetic.com/blog/cloud/getting-cloud-compliant-and-beyond/