Chính sách và nguyên tắc quản lý quyền truy cập

Chính sách

Chính sách về bảo mật đám mây đề cập đến một bộ quy tắc và nguyên tắc xác định cách người dùng nên truy cập và bảo vệ tài nguyên trong môi trường đám mây. Các chính sách này cung cấp một khuôn khổ để duy trì bảo mật, đảm bảo tuân thủ các quy định của ngành và giảm thiểu rủi ro tiềm ẩn.

Định dạng của một chính sách thường bao gồm:

- Tiêu đề cung cấp tên mô tả hoặc mã định danh cho chính sách
- Phạm vi của chính sách, xác định các nguồn lực, hệ thống hoặc cá nhân cụ thể mà chính sách áp dụng
- Mục tiêu của chính sách, hoặc mục tiêu và mục đích của nó
- Một tuyên bố chính sách liệt kê các quy tắc, thủ tục và hạn chế của chính sách
- Vai trò và trách nhiệm của các cá nhân và nhóm thực thi và tuân thủ chính sách

- Chi tiết về tuân thủ và thực thi hoặc các biện pháp được thực hiện để giám sát và đảm bảo tuân thủ chính sách
- Phần đánh giá và sửa đổi nêu rõ tần suất xem xét và cập nhật chính sách để duy trì tính phù hợp và hiệu quả

Chính sách nhà cung cấp dịch vụ và khách hàng quản lý

Các nhà cung cấp dịch vụ đám mây (CSP) thường có các chính sách bảo mật chi phối bảo mật chung của cơ sở hạ tầng, trung tâm dữ liệu và dịch vụ của họ. Các chính sách này đảm bảo mức độ bảo mật và bảo vệ cơ bản cho dữ liệu khách hàng. Chính sách của nhà cung cấp dịch vụ bao gồm nhiều khía cạnh khác nhau như bảo mật vật lý, bảo mật mạng, mã hóa dữ liệu, kiểm soát truy cập và ứng phó sự cố.

Ngoài các chính sách của nhà cung cấp dịch vụ, khách hàng có thể thực hiện các chính sách của riêng mình hay còn gọi là chính sách do khách hàng quản lý. Các chính sách này cho phép khách hàng điều chỉnh các biện pháp bảo mật theo yêu cầu, quy định của ngành và mức độ chấp nhận rủi ro. Các chính sách do khách hàng quản lý có thể bao gồm các biện pháp kiểm soát bảo mật bổ sung, hạn chế truy cập, các biện pháp bảo vệ dữ liệu và khung tuân thủ.

Bằng cách kết hợp nhà cung cấp dịch vụ và các chính sách do khách hàng quản lý, các tổ chức có thể thiết lập khung bảo mật toàn diện phù hợp với nhu cầu riêng của họ đồng thời hưởng lợi từ các biện pháp bảo mật cơ bản do nhà cung cấp dịch vụ đám mây cung cấp.

Nguyên tắc đặc quyền tối thiểu

Nguyên tắc đặc quyền tối thiểu là khái niệm then chốt trong kiểm soát truy cập nhằm giảm thiểu rủi ro truy cập trái phép hoặc vô tình lạm dụng tài nguyên. Nó quy định rằng các tổ chức chỉ nên cấp cho người dùng những quyền cần thiết tối thiểu cần thiết để thực hiện nhiệm vụ của họ. Bằng cách tuân theo nguyên tắc đặc quyền tối thiểu, các tổ chức sẽ hạn chế thiệt hại tiềm tàng do tài khoản người dùng bị xâm phạm gây ra.

Cấp độ truy cập của người dùng

Trong môi trường đám mây, cấp độ truy cập của người dùng khác nhau tùy thuộc vào vai trò và trách nhiệm của họ. Một số người dùng có thể chỉ cần quyền truy cập vào bảng điều khiển hoặc giao diện người dùng đồ họa (GUI) do nhà cung cấp dịch vụ đám mây cung cấp để quản lý và cấu hình tài nguyên. Những người dùng này tương tác với đám mây thông qua bảng điều khiển để thực hiện các tác vụ như cung cấp tài nguyên, giám sát và quản trị.

Mặt khác, người dùng tham gia phát triển phần mềm có thể yêu cầu quyền truy cập vào môi trường phát triển. Môi trường này bao gồm các công cụ, API và dịch vụ cần thiết để xây dựng, thử nghiệm và triển khai ứng dụng trên đám mây. Những người dùng này tương tác với cơ sở hạ tầng đám mây bằng API và giao diện dòng lệnh (CLI) thay vì chỉ dựa vào bảng điều khiển.

Tùy thuộc vào yêu cầu của tổ chức, một số người dùng nhất định có thể có quyền truy cập vào cả bảng điều khiển và môi trường phát triển, cho phép họ thực hiện nhiều nhiệm vụ và trách nhiệm hơn.

Quản lý danh tính và quyền truy cập (IAM)

Quản lý danh tính và quyền truy cập (IAM) cho phép các tổ chức quản lý và xác thực danh tính của người dùng cũng như quyền truy cập vào tài nguyên trong môi trường đám mây. Nó liên quan đến các quy trình và chính sách đảm bảo rằng chỉ những cá nhân được ủy quyền mới có đặc quyền truy cập vào các hệ thống, ứng dụng và dữ liệu nhạy cảm. IAM đơn giản hóa việc quản lý người dùng bằng cách tập trung các quy trình cấp phép, xác thực và ủy quyền cho người dùng, giúp việc cấp hoặc thu hồi quyền truy cập trở nên dễ dàng hơn khi cần. Quá trình này giúp các tổ chức tăng cường bảo mật, bảo vệ thông tin nhạy cảm, thực thi việc tuân thủ các quy định và hợp lý hóa các nhiệm vụ quản trị liên quan đến quyền truy cập của người dùng.

Chính sách mật khẩu tiêu chuẩn

Chính sách mật khẩu tiêu chuẩn dành cho người dùng đăng nhập vào đám mây phải tuân thủ các phương pháp hay nhất để đảm bảo bảo mật mật khẩu mạnh. Thông thường, chính sách mật khẩu bao gồm các yêu cầu về độ phức tạp của mật khẩu, chẳng hạn như độ dài tối thiểu và sự kết hợp giữa chữ hoa và chữ thường, số và ký tự đặc biệt. Chính sách cũng có thể xác định khoảng thời gian hết hạn mật khẩu, sau khoảng thời gian đó người dùng phải thay đổi mật khẩu của mình. Ngoài ra, việc thực thi lịch sử mật khẩu, tức là số lượng mật khẩu duy nhất bắt buộc được sử dụng trước khi sử dụng lại mật khẩu cũ, sẽ bổ sung thêm một lớp bảo vệ chống lại việc sử dụng lại mật khẩu. Các chính sách mật khẩu khác có thể bao gồm khóa tài khoản, xác thực đa yếu tố cũng như nhận thức và đào tạo người dùng. Các yêu cầu cụ thể của chính sách mật khẩu sẽ phụ thuộc vào nhu cầu, yêu cầu và đánh giá rủi ro của tổ chức.

Tiêu chuẩn nhà cung cấp nhận dạng (SAML, OpenID)

Tiêu chuẩn nhà cung cấp danh tính là các giao thức và khung xác định cách nhà cung cấp danh tính (IdP) và nhà cung cấp dịch vụ (SP) trao đổi thông tin nhận dạng và xác thực một cách an toàn. Các tiêu chuẩn này đảm bảo các phương pháp tiếp cận nhất quán và tiêu chuẩn hóa để xác thực và quản lý quyền truy cập. Hai tiêu chuẩn nhà cung cấp danh tính được sử dụng rộng rãi là:

- Ngôn ngữ đánh dấu xác nhận bảo mật (SAML) - SAML là một tiêu chuẩn dựa trên XML để trao đổi dữ liệu xác thực và ủy quyền giữa IdP và SP. Nó cho phép đăng nhập một lần (SSO) an toàn và liên kết danh tính. SAML cho phép người dùng xác thực một lần bằng IdP của họ và truy cập nhiều SP mà không cần xác thực riêng. Các xác nhận SAML chứa thông tin về danh tính và thuộc tính của người dùng mà SP dựa vào đó để cấp quyền truy cập vào tài nguyên của họ.
- OpenID Connect - OpenID Connect là một tiêu chuẩn hiện đại được xây dựng trên giao thức OAuth 2.0. Nó cung cấp một khuôn khổ để xác thực và liên kết danh tính. OpenID Connect cho phép người dùng xác thực bằng cách sử dụng nhà cung cấp OpenID đã chọn của họ và nhận mã thông báo ID chứa thông tin về danh tính của họ. Nhà cung cấp dịch vụ có thể sử dụng mã thông báo ID để xác thực người dùng và cung cấp quyền truy cập vào tài nguyên của họ.

Các tiêu chuẩn nhà cung cấp danh tính này cung cấp các giải pháp an toàn và có khả năng tương tác để quản lý xác thực và kiểm soát truy cập trong nhiều bối cảnh khác nhau, bao gồm môi trường đám mây, ứng dụng web và hệ thống doanh nghiệp. Chúng cho phép các tổ chức thiết lập mối quan hệ tin cậy giữa nhà cung cấp danh tính và nhà cung cấp dịch vụ, đơn giản hóa trải nghiệm xác thực người dùng và tăng cường bảo mật bằng cách tập trung quản lý danh tính.