Authorization

1. Các khái niệm cơ bản.

- Authorization là qua trình cho phép thực thế có quyền truy cấp vào 1 thứ gì đó hoặc thực hiện các h ành động cụ thể trong hệ thống máy tính.

- việc xác đinh uỷ quyền cũng là xác đinh nhiệm vụ trong 1 hệ thống và đảm bảo tính tiêng tư trong hệ thống.

2. hoạt động.

- bước 1 xác minh danh tính : Sau khi xác thực danh tính của người dùng, hệ thống sẽ tham khảo chính sách cấp phép để quyết định tài nguyên và hành động nào mà người dùng được phép truy cập.

- bước 2 Chính sách truy cập : Chính sách ủy quyền được xác định dựa trên các yêu cầu bảo mật của tổ chức và thường được quản lý thông qua các khuôn khổ như Kiểm soát truy cập dựa trên vai trò (RBAC), Kiểm soát truy cập dựa trên thuộc tính (ABAC) hoặc Kiểm soát truy cập dựa trên mối quan hệ (ReBAC). Các chính sách này thiết lập quyền cho nhiều vai trò, thuộc tính hoặc mối quan hệ của người dùng.

- bước 3 Phân công quyền : Hệ thống phân công quyền theo các chính sách đã xác định. Ví dụ, trong RBAC, người dùng được phân công các vai trò như 'quản trị viên' hoặc 'biên tập viên', đi kèm với các quyền truy cập được xác định trước.

- bước 4 Cơ chế kiểm soát truy cập : Khi người dùng cố gắng truy cập một tài nguyên, hệ thống kiểm soát truy cập sẽ kiểm tra quyền của người dùng so với hành động được yêu cầu. Nếu quyền của người dùng bao gồm hành động được yêu cầu, quyền truy cập sẽ được cấp; nếu không, quyền truy cập sẽ bị từ chối.

- bước 5 Kiểm tra và giám sát : Việc giám sát và ghi lại liên tục các hành động ủy quyền giúp phát hiện các nỗ lực truy cập trái phép và đảm bảo tuân thủ các chính sách bảo mật.

3. chiến lược và kỹ thuật.

- Kiểm soát truy cập dựa trên vai trò (RBAC)

Cơ chế RBAC cho phép hoặc hạn chế quyền truy cập của người dùng theo vai trò của họ trong tổ chức. Nó cung cấp cho người dùng quyền truy cập vào dữ liệu và

ứng dụng cần thiết để thực hiện công việc của họ đồng thời giảm thiểu rủi ro của các hoạt động trái phép như truy cập vào dữ liệu nhạy cảm.

- Kiểm soát truy cập dựa trên thuộc tính (ABAC)

ABAC cho phép bạn xác định quyền truy cập và đặc quyền dựa trên các thuộc tính (hoặc đặc điểm) thay vì vai trò. Nó giúp bảo vệ các đối tượng như thiết bị mạng, tài nguyên CNTT và dữ liệu khỏi các hành động trái phép và người dùng không có các đặc điểm được chấp thuận theo chính sách bảo mật của tổ chức.

- Kiểm soát truy cập dựa trên mối quan hệ (ReBAC)

ReBAC áp dụng các quyết định truy cập theo mối quan hệ giữa các chủ thể như người dùng, ứng dụng và thiết bị. Khi một chủ thể yêu cầu truy cập vào một tài nguyên, cơ chế ReBAC sẽ cấp hoặc từ chối quyền truy cập theo mối quan hệ mà chủ thể đó có.

- Mã thông báo web JSON (JWT)

JSON Web Token (JWT) là một tiêu chuẩn mở xác định cách truyền thông tin an toàn giữa các bên như đối tượng JSON. Nó xác minh thông tin bằng cách ký kỹ thuật số. JWT nhỏ gọn và độc lập. Bạn có thể ký JWT bằng cặp khóa công khai/riêng tư thông qua RSA hoặc ECDSA hoặc bí mật thông qua thuật toán HMAC.

4. khó khăn trong uỷ quyền.

- Sự phức tạp trong quản lý chính sách

Khi các tổ chức phát triển và cơ sở hạ tầng CNTT của họ trở nên tinh vi hơn, việc quản lý các chính sách kiểm soát truy cập có thể trở nên cực kỳ phức tạp. Sự phức tạp này phát sinh từ nhu cầu cân bằng các yêu cầu truy cập khác nhau giữa các phòng ban, vai trò và dự án khác nhau. Ví dụ, các nhóm khác nhau trong một tổ chức có thể yêu cầu truy cập vào các tập hợp tài nguyên khác nhau và mỗi nhóm có thể có các cấp độ quyền truy cập khác nhau.

Ngoài ra, các yêu cầu về quy định thường đòi hỏi các biện pháp kiểm soát truy cập chi tiết, thêm một lớp phức tạp nữa vào việc quản lý chính sách. Đảm bảo rằng tất cả các chính sách này được triển khai đúng cách và thực thi nhất quán là một thách thức đáng kể, đặc biệt là khi sử dụng các khuôn khổ như Kiểm soát truy cập dựa trên thuộc tính (ABAC), trong đó nhiều thuộc tính và điều kiện phải được quản lý.

- Khả năng mở rộng

Hệ thống ủy quyền phải có khả năng mở rộng hiệu quả khi tổ chức phát triển. Điều này có nghĩa là xử lý số lượng người dùng, tài nguyên và yêu cầu truy cập ngày càng tăng mà không ảnh hưởng đến hiệu suất hoặc bảo mật.

Các vấn đề về khả năng mở rộng có thể phát sinh dưới nhiều hình thức khác nhau, chẳng hạn như sự chậm trễ trong quá trình ra quyết định truy cập, tăng tải trên máy chủ và khó khăn trong việc duy trì danh sách kiểm soát truy cập được cập nhật. Trong các doanh nghiệp lớn và môi trường đám mây, bản chất năng động và thường không thể đoán trước của các yêu cầu mở rộng làm phức tạp thêm việc triển khai các cơ chế ủy quyền hiệu quả. Thách thức này đặc biệt rõ rệt trong các môi trường mà hàng nghìn quyết định truy cập phải được đưa ra theo thời gian thực.

- Tích hợp với các hệ thống hiện có

Việc tích hợp các cơ chế ủy quyền mới với các hệ thống cũ là một thách thức to lớn. Các hệ thống cũ thường không được thiết kế với các yêu cầu kiểm soát truy cập hiện đại, dẫn đến các vấn đề tương thích tiềm ẩn. Các hệ thống cũ này có thể sử dụng các giao thức lỗi thời hoặc không tương thích, khiến việc triển khai các giải pháp ủy quyền hiện đại trở nên khó khăn nếu không có những thay đổi đáng kể.

Ngoài ra, quá trình tích hợp phải đảm bảo rằng chức năng hiện có không bị gián đoạn, thường đòi hỏi phải thử nghiệm rộng rãi và có khả năng phát triển tùy chỉnh. Quá trình này có thể tốn thời gian và tài nguyên, tạo ra rào cản đáng kể đối với việc cập nhật cơ sở hạ tầng ủy quyền.

- Trải nghiệm người dùng

Việc cân bằng các biện pháp bảo mật mạnh mẽ với trải nghiệm người dùng liền mạch là một nhiệm vụ phức tạp. Các biện pháp kiểm soát ủy quyền quá nghiêm ngặt có thể gây khó chịu cho người dùng, dẫn đến giảm năng suất và các giải pháp thay thế tiềm ẩn gây ảnh hưởng đến bảo mật.

Ví dụ, nếu người dùng thường xuyên gặp phải tình trạng từ chối truy cập hoặc quy trình xác thực đa yếu tố rườm rà, họ có thể tìm kiếm các phương pháp kém an toàn hơn để đạt được mục tiêu của mình. Đạt được sự cân bằng phù hợp không chỉ bao gồm việc triển khai các biện pháp kiểm soát bảo mật hiệu quả mà còn thiết kế các

giao diện và quy trình trực quan và thân thiện với người dùng, không cản trở khả năng thực hiện nhiệm vụ của người dùng một cách hiệu quả.