Tópicos Especiais - Segurança da Informação

Gerenciamento de Identidade e Acesso

O que é IAM ?

O Gerenciamento de Identidade e Acesso (IAM) é crucial para a segurança da informação, envolvendo processos, políticas e tecnologias para controlar o acesso dos usuários a recursos críticos. IAM engloba autenticação, autorização e administração, garantindo que a identidade certa tenha acesso correto aos recursos. Isso protege contra ameaças internas e externas, reduzindo riscos de violações e garantindo conformidade com regulamentos.

IAM é baseado na restrição e controle de acesso conforme políticas, práticas de segurança e requisitos de conformidade, proporcionando acesso seguro e eficiente aos recursos enquanto protege contra acessos não autorizados.

Com o avanço da tecnologia e o aumento da complexidade dos ambientes de TI, o IAM tornou-se ainda mais crucial. Ele permite que as organizações enfrentam desafios contemporâneos, como a gestão de identidades em ambientes híbridos e em nuvem, a implementação de autenticação forte e o gerenciamento de acessos privilegiados, garantindo que a segurança da informação permaneça robusta em um cenário em constante evolução.

Autenticação

A autenticação é um processo crítico que valida a identidade de um usuário, dispositivo ou sistema. Ela é um componente fundamental da segurança cibernética, garantindo que apenas entidades autorizadas tenham acesso aos sistemas de informação.

A autenticação é uma parte importante do gerenciamento de identidade e acesso (IAM), que determina quem pode visualizar os dados e o que eles podem fazer com eles. Mas também se aplica a muitas outras áreas de segurança, incluindo: TLS (Transport Layer Security), APIs, e-mail, entre outros.

Portanto, a autenticação é uma comprovação de identidade que pode servir no contexto de segurança de informação para autenticar em sistemas e acessar informações privadas e locais com acesso restrito, entre outras opções.

Princípios da Autenticação

Os princípios de autenticação se baseiam em três conceitos: **conhecimento**, **posse** e **inerência**. Esses conceitos são usados para verificar a identidade de um usuário ou sistema que deseja acessar um recurso protegido, como um site, um aplicativo ou uma rede. Cada conceito tem suas vantagens e desvantagens, e podem ser combinados para fornecer diferentes níveis de segurança.

Conhecimento: Este princípio se refere a algo que o usuário sabe. Isso pode ser uma senha, um PIN ou uma resposta a uma pergunta de segurança. É uma informação que é exclusiva para o usuário e que, idealmente, só ele conhece.

A vantagem desse princípio é que ele é simples e fácil de usar, pois não requer nenhum dispositivo ou hardware adicional. A desvantagem é que ele é vulnerável a ataques de força bruta, phishing, engenharia social ou esquecimento.

Posse: Este princípio se refere a algo que o usuário possui. Isso pode ser um token de hardware, um cartão inteligente ou um dispositivo móvel. A ideia é que o objeto em posse do usuário forneça um nível adicional de autenticação.

A vantagem desse princípio é que ele é mais seguro do que o conhecimento, pois dificulta que um atacante obtenha acesso ao objeto. A desvantagem é que ele pode ser perdido, roubado, danificado ou clonado.

Inerência: Este princípio se refere a algo que é inerente ao usuário. Isso pode ser uma característica biométrica, como uma impressão digital, reconhecimento facial ou de voz. Estes são aspectos únicos para cada indivíduo, tornando-os métodos de autenticação muito seguros.

A vantagem desse princípio é que ele é conveniente e difícil de falsificar, pois não depende de memorizar ou digitar informações, mas sim de apresentar alguma parte do corpo. A desvantagem é que ele pode ter implicações de privacidade, pois os dados biométricos podem ser usados para outros fins, e requer hardware especializado para capturar e verificar as características.

Métodos de Autenticação

Existem vários métodos de autenticação disponíveis, cada um com suas próprias características, vantagens e desvantagens. A escolha do método mais adequado depende de vários fatores, como o nível de segurança necessário, a conveniência para o usuário e os recursos disponíveis. Alguns dos métodos mais comuns são:

Autenticação por senha:

Autenticação de Dois fatores:

Autenticação Biométrica:

Autenticação Baseada em Certificados:

Autenticação por Sessão:

Autenticação Baseada em Chave Pública:

Autenticação por senha: Este é o método mais simples e difundido, onde os usuários precisam fornecer um nome de usuário e uma senha para acessar um sistema. A senha é uma informação que somente o usuário deveria conhecer, mas pode ser facilmente roubada, esquecida ou adivinhada por terceiros. Por isso, é recomendado usar senhas fortes, complexas e diferentes para cada serviço.

Autenticação de dois fatores (2FA): Este método requer que os usuários forneçam duas formas de identificação, normalmente algo que eles conhecem (como uma senha) e algo que eles têm (como um token ou código enviado para o seu celular). Isso aumenta a segurança, pois dificulta que alguém que tenha apenas a senha possa acessar o sistema. No entanto, pode ser mais inconveniente para o usuário, que precisa ter o dispositivo adicional disponível e digitar o código a cada acesso.

Autenticação biométrica: Este método usa características físicas ou comportamentais únicas dos usuários, como impressões digitais, reconhecimento facial ou de voz. É muito seguro e conveniente, pois não depende de memorizar ou digitar informações, mas sim de apresentar alguma parte do corpo. No entanto, pode ter implicações de privacidade, pois os dados biométricos podem ser usados para outros fins, e requer hardware especializado para capturar e verificar as características.

Autenticação baseada em certificados: Este método usa certificados digitais para autenticar usuários ou sistemas. Os certificados são emitidos por uma Autoridade de Certificação (CA) e contém informações sobre a identidade do titular do certificado, bem como uma chave pública que pode ser usada para criptografar e assinar dados. O usuário ou sistema precisa ter uma chave privada correspondente, que é mantida em segredo, para provar que possui o certificado. Este método oferece alta segurança, mas a gestão de certificados pode ser complexa e requer infraestrutura adequada.

Autenticação por sessão: Este foi um dos primeiros métodos de autenticação, criado no início do desenvolvimento das aplicações web. Neste método, o usuário fornece suas credenciais (como usuário e senha) uma vez, e recebe um identificador de sessão, que é armazenado em um cookie no navegador. Esse identificador é usado para validar o usuário em cada requisição subsequente, sem precisar pedir as credenciais novamente. O identificador é associado a um estado de sessão no servidor, que contém as informações do usuário. Este método é simples e prático, mas pode ter problemas de escalabilidade, pois o servidor precisa manter o estado de cada sessão ativa.

Autenticação baseada em chave pública: Este é um método que usa um par de chaves, uma pública e uma privada, para autenticar usuários. A chave pública é divulgada para todos, enquanto a chave privada é mantida em segredo pelo usuário. O usuário pode usar sua chave privada para assinar uma mensagem, que pode ser verificada por qualquer um que tenha sua chave pública. Assim, o usuário prova que é o dono da chave pública, sem revelar sua chave privada. Este método é muito seguro, mas requer que as chaves sejam geradas, distribuídas e armazenadas de forma segura.

Tendências e Inovações

- Autenticação sem senha: Essa tendência visa eliminar o uso de senhas tradicionais, que podem ser facilmente roubadas ou esquecidas, e substituí-las por métodos mais seguros e convenientes, como biometria, tokens, senhas de uso único e links mágicos.

Tendências e Inovações

- Inteligência artificial e aprendizado de máquina: Essas tecnologias permitem analisar grandes volumes de dados em tempo real e identificar padrões e comportamentos suspeitos. Elas podem ser usadas para melhorar a detecção e prevenção de ameaças, bem como para oferecer uma autenticação contínua baseada no comportamento do usuário. Essas tecnologias também podem ser aplicadas para criar sistemas de autenticação adaptativos, que ajustam o nível de segurança de acordo com o contexto e o risco de cada situação.

Tendências e Inovações

- Autenticação multifatorial e biometria: Esses métodos combinam diferentes fatores de autenticação, como algo que o usuário sabe, possui ou é, para garantir uma verificação de identidade mais robusta. A biometria usa características físicas ou comportamentais únicas do usuário, como impressões digitais, reconhecimento facial ou de voz, para autenticar o usuário. Esses métodos podem ser integrados com outras tecnologias, como a nuvem e o 5G, para oferecer uma autenticação mais rápida e conveniente.

Tendências e Inovações

- Zero Trust Security: Esse modelo de segurança assume que nenhum usuário ou dispositivo pode ser confiável automaticamente, e requer que eles sejam autenticados e autorizados a cada acesso. Esse modelo reduz o risco de violações de segurança e aumenta a confiabilidade da autenticação. Esse modelo também implica em uma mudança de paradigma, onde a segurança não é mais baseada em perímetros, mas sim em identidades.

Autorização autorização é o processo que ocorre após a autenticação. Uma vez que um usuário é autenticado, o sistema precisa determinar quais ações são permitidas para esse usuário. Isso é feito através de políticas de autorização, que definem as permissões de um usuário, como ler, escrever, executar, criar ou deletar arquivos ou registros.

Existem diferentes tipos de políticas de autorização, classificadas de acordo com os critérios usados para atribuir as permissões:

Política Baseada em Identidade: As permissões são atribuídas diretamente aos usuários ou grupos de usuários, com base em suas identidades. Por exemplo, um usuário pode ter permissão para ler e escrever em um arquivo específico, enquanto outro usuário pode ter apenas permissão para ler o mesmo arquivo.

Política Baseada em Atributo: As permissões são atribuídas com base em atributos dos usuários, dos objetos ou do contexto. Por exemplo, um usuário pode ter permissão para acessar um recurso se ele tiver um determinado cargo, se o recurso tiver uma determinada classificação ou se o acesso ocorrer em um determinado horário.

Política Baseada em Função: As permissões são atribuídas com base nas funções que os usuários desempenham no sistema. Por exemplo, um usuário pode ter permissão para executar uma ação se ele for um administrador, um gerente ou um funcionário.

Política Baseada em Regra: As permissões são atribuídas com base em regras lógicas que especificam as condições para o acesso. Por exemplo, um usuário pode ter permissão para acessar um recurso se ele satisfizer uma expressão booleana que envolva seus atributos, os atributos do recurso ou o contexto.

Modelos de Controle de Acesso

Existem vários modelos de controle de acesso que os sistemas podem usar para implementar as políticas de autorização. Cada modelo tem suas vantagens e desvantagens, e a escolha do modelo mais adequado depende dos requisitos de segurança e da complexidade do sistema:

Controle de Acesso Baseado em Funções (RBAC):

Controle de Acesso Baseado em Atributos (ABAC):

Controle de Acesso Discricionário (DAC):

Controle de Acesso Obrigatório (MAC):

Gestão de Identidade (IAM)

A gestão de identidade e acesso (IAM) é uma forma de garantir que pessoas e entidades com identidades digitais tenham o nível certo de acesso aos recursos da empresa, como redes e bancos de dados. As funções do usuário e os privilégios de acesso são definidos e gerenciados por meio de um sistema de IAM, que pode incluir processos, políticas e tecnologias.

Provisionamento: é a fase em que as identidades de usuário são criadas e atribuídas a funções e permissões adequadas, de acordo com as necessidades do negócio e as políticas de segurança.

Autenticação: é a fase em que os usuários provam suas identidades ao sistema, por meio de métodos como senhas, biometria ou tokens.

Autorização: é a fase em que o sistema verifica se os usuários têm permissão para acessar os recursos solicitados, de acordo com as políticas de controle de acesso.

Auditoria: é a fase em que o sistema monitora e registra as atividades de acesso dos usuários, para verificar se há violações ou anomalias, e para gerar relatórios de conformidade.

Automação no IAM

A automação no IAM pode trazer vários benefícios para as empresas, tais como:

Redução de custos operacionais: A automação pode reduzir o tempo e o esforço necessários para gerenciar as identidades e os acessos dos usuários, diminuindo a dependência de recursos humanos e evitando gastos desnecessários com licenças, infraestrutura e manutenção.

Melhoria da experiência do usuário: A automação pode proporcionar uma experiência de usuário mais ágil e conveniente, permitindo que os usuários solicitem, recebam e gerenciem seus próprios acessos de forma rápida e fácil, sem a necessidade de intervenção manual ou aprovações demoradas.

Automação no IAM

Aumento da segurança e da conformidade: A automação pode aumentar a segurança e a conformidade, garantindo que as políticas de acesso sejam aplicadas de forma consistente e que os usuários tenham apenas os acessos necessários para suas funções. A automação também pode facilitar a detecção e a correção de violações de acesso, bem como a geração de relatórios e evidências para auditorias internas e externas.

Alguns exemplos de ferramentas de automação no IAM são:

Robotic Process Automation (RPA): É uma tecnologia que usa robôs de software para automatizar processos de negócio baseados em regras, como a criação, a modificação e a exclusão de contas de usuário.

Identity Governance and Administration (IGA): É uma solução que permite gerenciar o ciclo de vida das identidades e dos acessos dos usuários, incluindo o provisionamento, a revisão, a certificação e o desprovisionamento de acessos, bem como a gestão de funções, políticas e riscos.

Privileged Access Management (PAM): É uma solução que permite controlar e monitorar os acessos privilegiados dos usuários, como administradores, executivos e terceiros, que têm permissões para acessar recursos críticos e sensíveis da empresa.