1

Controles de Acesso

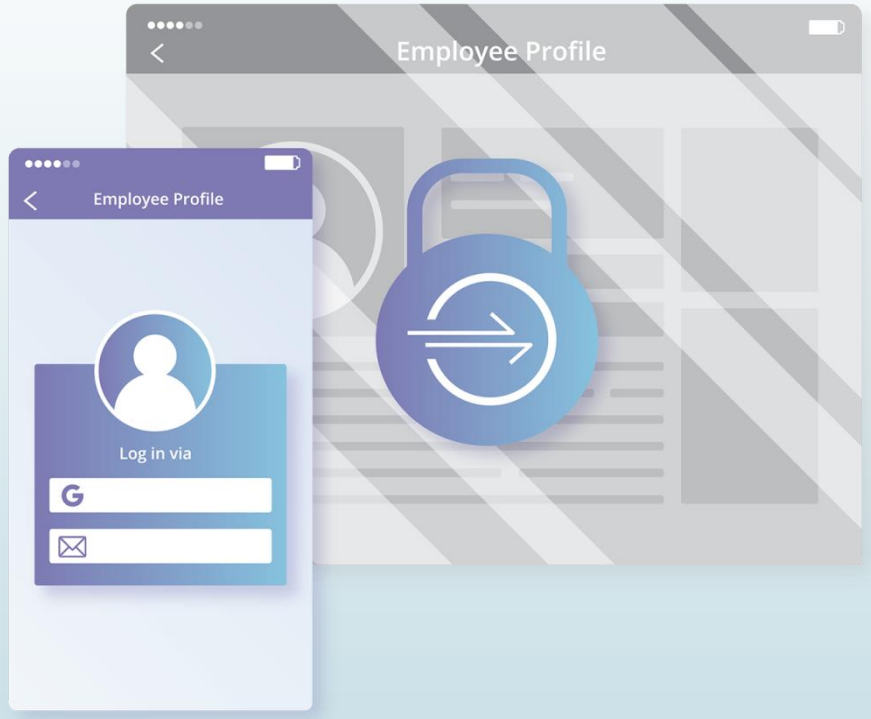
Segurança e Auditoria de Sistemas

Segurança e Auditoria de Sistemas

Controles de Acesso

O que é controle de acesso?

Controle de acesso é um termo de segurança usado para se referir a um conjunto de políticas para restringir o acesso a informações, ferramentas e locais físicos.



Segurança e Auditoria de Sistemas

Controles de Acesso

O que é controle de acesso físico?

Embora este artigo se concentre no controle de acesso à informação, o controle de acesso físico é uma comparação útil para entender o conceito geral.

O controle de acesso físico é um conjunto de políticas para controlar quem tem acesso a um local físico. Exemplos do mundo real de controle de acesso físico incluem:

- Seguranças de bar
- Catracas de metrô
- Agentes alfandegários de aeroportos
- Scanners de cartões de acesso ou crachás em escritórios corporativos

Segurança e Auditoria de Sistemas

Controles de Acesso

O que é controle de acesso físico?

Em todos esses exemplos, uma pessoa ou dispositivo está seguindo um conjunto de políticas para decidir quem tem acesso a um local físico restrito. Por exemplo, um scanner de cartão de acesso de um hotel só concede acesso a hóspedes autorizados que tenham uma chave do hotel.

Segurança e Auditoria de Sistemas

Controles de Acesso

O que é controle de acesso a informações?

O controle de acesso a informações restringe o acesso aos dados e ao software utilizado para manipular esses dados. Alguns exemplos são:

- Entrar em um notebook usando uma senha
- Desbloquear um smartphone com a digitalização da impressão digital
- Acessar remotamente a rede interna de um empregador usando uma VPN

Em todos estes casos, o software é usado para autenticar e conceder autorização aos usuários que precisam acessar informações digitais. **Autenticação e autorização** são componentes integrais do controle de acesso às informações.

Segurança e Auditoria de Sistemas

Controles de Acesso

Qual é a diferença entre autenticação e autorização

Autenticação é a prática de segurança de confirmar que alguém é quem afirma ser, enquanto a **autorização** é o processo de determinar qual nível de acesso cada usuário tem.

Por exemplo, pense em um viajante fazendo check-in em um hotel. Quando ele se registra na recepção, é solicitado que apresentem um passaporte para verificar se são a pessoa cujo nome consta da reserva. Este é um exemplo de autenticação.

Segurança e Auditoria de Sistemas

Controles de Acesso

Qual é a diferença entre autenticação e autorização

Assim que o funcionário do hotel autenticar o hóspede, ele recebe um cartão de acesso com privilégios limitados. Este é um exemplo de autorização. O cartão de acesso do hóspede concede acesso ao quarto, ao elevador de hóspedes e à piscina — mas não aos quartos de outros hóspedes ou ao elevador de serviço. Os funcionários do hotel, por outro lado, estão autorizados a acessar mais áreas do hotel do que os hóspedes.

Segurança e Auditoria de Sistemas

Controles de Acesso

Qual é a diferença entre autenticação e autorização

Os sistemas de computador e de rede têm controles de autenticação e autorização semelhantes. Quando um usuário faz login em seu e-mail ou conta bancária on-line, ele usa uma combinação de login e senha que apenas ele deveria saber. O software usa essas informações para autenticar o usuário. Alguns aplicativos têm requisitos de autorização muito mais rígidos do que outros; enquanto uma senha é suficiente para alguns, outros podem exigir **autenticação de dois fatores** ou uma confirmação biométrica, como digitalização de impressão digital ou identificação facial.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os principais tipos de controle de acesso?

Após a conclusão do processo de autenticação, a autorização do usuário pode ser determinada de várias maneiras:

- **Controle de acesso obrigatório (MAC)**

  Controle de acesso obrigatório estabelece políticas de segurança rígidas para usuários individuais e os recursos, sistemas ou dados que eles têm permissão para acessar. Essas políticas são controladas por um administrador; os usuários individuais não têm autoridade para definir, alterar ou revogar permissões de uma forma que contradiga as políticas existentes.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os principais tipos de controle de acesso?

- **Controle de acesso obrigatório (MAC)**

  Nesse sistema, tanto o sujeito (usuário) quanto o objeto (dados, sistema ou outro recurso) devem receber atributos de segurança semelhantes para interagirem entre si. Voltando ao exemplo anterior, o presidente do banco não só precisaria da autorização de segurança correta para acessar os arquivos de dados do cliente, mas o administrador do sistema precisaria especificar que esses arquivos podem ser visualizados e alterados pelo presidente. Embora esse processo possa parecer redundante, ele garante que os usuários não possam executar ações não autorizadas simplesmente obtendo acesso a determinados dados ou recursos.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os principais tipos de controle de acesso?

- **Controle de acesso baseado em função (RBAC):**

O controle de acesso baseado em função estabelece permissões com base em grupos (conjuntos definidos de usuários, como funcionários do banco) e funções (conjuntos definidos de ações, como aqueles que um caixa de banco ou um gerente de agência pode realizar). Os indivíduos podem executar qualquer ação atribuída à sua função e podem receber várias funções conforme necessário. Assim como o MAC, os usuários não têm permissão para alterar o nível de controle de acesso atribuído à sua função.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os principais tipos de controle de acesso?

- **Controle de acesso baseado em função (RBAC):**

Por exemplo, qualquer funcionário do banco designado para a função de caixa do banco pode receber autorização para processar transações de contas e abrir novas contas de clientes. Um gerente de agência, por outro lado, pode ter várias funções, que o autorizam a processar transações de contas, abrir contas de clientes, atribuir a função de caixa de banco a um novo funcionário e assim por diante.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os principais tipos de controle de acesso?

- **Controle de acesso discricionário (DAC)**

Uma vez que um usuário recebe permissão para acessar um objeto (geralmente por um administrador do sistema ou por meio de uma lista de controle de acesso existente), ele pode conceder acesso a outros usuários conforme necessário. No entanto, isso pode introduzir vulnerabilidades de segurança, pois os usuários podem determinar as configurações de segurança e compartilhar permissões sem supervisão estrita do administrador do sistema.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os principais tipos de controle de acesso?

- **Controle de acesso discricionário (DAC)**

Ao avaliar qual método de autorização de usuário é mais apropriado para uma organização, as necessidades de segurança devem ser levadas em consideração. Normalmente, as organizações que exigem um alto nível de confidencialidade de dados (por exemplo, organizações governamentais, bancos, etc.) optarão por formas mais rigorosas de controle de acesso, como MAC, enquanto aquelas que favorecem mais flexibilidade e permissões baseadas em usuários ou funções tenderão a sistemas RBAC e DAC.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os métodos para implementar o controle de acesso?

Uma ferramenta popular para controle de acesso a informações é uma rede privada virtual (VPN). Uma VPN é um serviço que permite que usuários remotos acessem a internet como se estivessem conectados a uma rede privada. As redes corporativas geralmente usam VPNs para gerenciar o controle de acesso à sua rede interna em uma distância geográfica.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os métodos para implementar o controle de acesso?

Por exemplo, se uma empresa tem um escritório em São Francisco e outro escritório em Nova York, bem como funcionários remotos espalhados pelo mundo, eles podem usar uma VPN para que todos os funcionários possam fazer login com segurança em sua rede interna, independentemente de sua localização física. Conectar-se à VPN também ajudará a proteger os funcionários contra ataques de invasores intermediários se estiverem conectados a uma rede Wi-Fi pública.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os métodos para implementar o controle de acesso?

As VPNs também apresentam algumas desvantagens. Por exemplo, as VPNs afetam negativamente a performance. Quando conectado a uma VPN, cada pacote de dados que um usuário envia ou recebe precisa percorrer uma distância extra antes de chegar ao seu destino, pois cada solicitação e resposta precisa atingir o servidor VPN antes de chegar ao seu destino. Esse processo geralmente aumenta a latência.

Segurança e Auditoria de Sistemas

Controles de Acesso

Quais são os métodos para implementar o controle de acesso?

As VPNs geralmente fornecem uma abordagem de tudo ou nada para a segurança da rede. As VPNs são ótimas para fornecer autenticação, mas não são ótimas para fornecer controles de autorização granulares. Se uma organização deseja conceder diferentes níveis de acesso a diferentes funcionários, ela precisa usar várias VPNs. Isso cria muita complexidade e também não atende aos requisitos de segurança Zero Trust.

Segurança e Auditoria de Sistemas

Controles de Acesso

O que é segurança zero trust?

A segurança Zero Trust é um modelo de segurança de TI que requer verificação de identidade rigorosa para todas as pessoas e dispositivos que tentam acessar recursos em uma rede privada, independentemente de estarem dentro ou fora do perímetro de rede. As redes Zero Trust também utilizam a microssegmentação. Microssegmentação é a prática de dividir os perímetros de segurança em pequenas zonas para manter o acesso separado para partes separadas da rede.

Referências

https://www.cloudflare.com/pt-br/learning/access-management/what-is-access-control/#:~:text=O%20controle%20de%20acesso%20a,a%20digitaliza%C3%A7%C3%A3o%20da%20impress%C3%A3o%20digital