1.Requisitos de negócio para o controle de acesso

O dono do negócio é a pessoa responsável por um processo, subprocesso ou atividade de negócio. Essa responsabilidade inclui a definição de quem pode ter acesso aos ativos, incluindo ativos de informação, e sob quais condições. Os requisitos podem vir de objetivos do negócio, legais e outros requisitos regulatórios. Uma avaliação de risco deve ser usada para determinar o quão estritos esses controles de acesso devem ser, visando limitar os riscos identificados relacionados à obtenção de acesso a ativos. Os controles de acesso são uma combinação de controles de acesso lógico, relacionados a sistemas de informação, e controles de acesso físico.

Uma autorização consiste em um conjunto de permissões. Tais permissões podem ser muito simples ou também podem ser muito complexas. No último caso, a autorização de usuários requer ao menos permissão para ler faturas de fornecedores, juntamente com permissões para fazer pagamentos bancários com base nas faturas. Alguns exemplos de tipos de acesso que devem ser levados em consideração ao definir controles de acesso são:

- Acesso a redes e serviços de rede
- Acesso a aplicações de negócio
- Acesso a equipamentos de TI
- Acesso à informação

2.Gestão de acesso do usuário

A gestão de acesso do usuário incorpora as atividades que são requeridas para prevenir que ativos sejam acessados por usuários não autorizados e garantir que estes sejam acessados somente por usuários autorizados. Para isso, é necessário ter as seguintes atividades:

- Registro e cancelamento de registro de usuário
- Provisionamento de acesso de usuário
- Gestão de informações secretas de autenticação de usuários
- Revisão dos direitos de acesso de usuário
- Remoção ou ajuste dos direitos de acesso

Conceder acesso a usuários autorizados envolve uma série de etapas que incluem a identificação do usuário, a autenticação deste usuário e a autorização do usuário para acessar um ativo. Identificação é o primeiro passo no processo de concessão de acesso. Na identificação, uma pessoa apresenta um token. O sistema então, precisa determinar se o token é autêntico. Para determinar a autenticidade de um nome de usuário, o sistema verifica se tal nome existe dentro do sistema. Se o nome de

usuário existir, é solicitada ao usuário uma senha. O sistema testa se a senha está registrada para o nome de usuário fornecido. Se ambos os testes forem válidos, o usuário será autenticado.

3.Responsabilidade do usuário

Para que o controle de acesso funcione, é fundamental que os usuários conheçam suas responsabilidades em termos de manter as informações e os ativos seguros e protegidos. Para conseguir isso, os usuários devem ser responsáveis por suas próprias informações de autenticação, salvaguardando essas informações. Em algumas organizações, são usados tokens para se logar na rede. Os usuários devem estar cientes de que precisam ter cuidado para que seu token não seja perdido ou roubado.

4.Acesso a sistemas e aplicações

Ao configurar um sistema de controle de acesso, deve-se levar em conta quem precisa do acesso à informação. Restringir o acesso à informação é sempre um ato de equilíbrio. Restringir o acesso à informação de forma demasiadamente rigorosa geralmente faz com que os usuários sejam impedidos de desempenhar as suas tarefas. Por outro lado, não estabelecer restrições suficientes ao acesso à informação significa uma maior chance de que pessoas não autorizadas possam acessar informações a que não se deve ter acesso. Ambos efeitos negativos para a organização.

Procedimentos seguros de logon também fazem parte dos controles de acesso a sistemas e aplicativos. O objetivo é ajudar o usuário a fazer logon e não dar nenhuma informação útil a um atacante. Medidas que podem ser tomadas, por exemplo são, não mostrar um nome padrão de usuário e, se o nome do usuário ou senha forem inseridos incorretamente, então o sistema não deve informar qual dos dois estava incorreto, de forma a não ajudar um atacante a determinar se um sistema ou aplicativo é o que ele ou ela está procurando.

Para ajudar os usuários a detectar se outra pessoa está usando sua conta, uma mensagem pode ser exibida, depois de feito o login com êxito, indicando a última vez que houve um login bem sucedido e também mostra quaisquer tentativas mal sucedidas de login. Normalmente, um usuário sabe quando fez login e essas informações podem ser úteis para a detecção de qualquer uso suspeito de uma conta.

A fim de manter as senhas seguras, pode ser usado um sistema de gerenciamento de senhas. Um bom sistema de gerenciamento pode ajudar um usuário a manter suas senhas. Outra forma de manter seguros os sistemas de controle de acesso é restringir o uso de programas utilitários privilegiados, tais como verificadores de senha e ferramentas usadas por administradores para manter o sistema. Normalmente, esses utilitários têm uma funcionalidade adicional que, nas mãos de um usuário não qualificado, pode levar a sérios problemas de sistema e nas mãos de um atacante pode levar a um comprometimento do sistema.

Para manter aplicações e sistemas seguros contra alterações não autorizadas ou acidentais, é importante também ter controles de acesso rígidos ao código-fonte e a informações afins. Outra razão para ter um rígido controle de acesso ao código-fonte é proteger qualquer propriedade intelectual que seja usada para desenvolver sistemas e aplicativos.

4.1 Formas de controle de acesso lógico

Vários conceitos diferentes estão disponíveis para implementação de um controle de acesso em um sistema automatizado. O tipo de controle de acesso que deve ser aplicado a um ativo precisa ser determinado pelo seu proprietário. Uma vez escolhido o tipo de controle de acesso, é necessário que este seja implementado pelo desenvolvedor ou administrador do sistema.

4.2 Controle de Acesso Discricionário (DAC)

O dono dos dados e os usuários individuais são capazes de definir qual acesso será permitido aos seus dados independente da política, ao seu critério. A principal vantagem do DAC é ser muito flexível do ponto de vista do usuário. A desvantagem é que esta forma de controle de acesso não é útil em ambientes onde os requisitos de conformidade são muito rigorosos. Isso é especialmente verdade se o usuário que está concedendo o acesso não é o dono do ativo.

Para se adequar aos requisitos de conformidade, uma organização deve ser capaz de provar que as informações são tratadas de acordo com as políticas estabelecidas. Isso deve ser motivo de preocupação para o dono do ativo, uma vez que ele/ela não pode assegurar que o sistema automatizado opera de acordo com essas políticas. Como resultado, os sistemas que trabalham com essa forma flexível de controle de acesso são geralmente difíceis de auditar. A principal razão para essa dificuldade é que, com o CAD, cada usuário toma decisões sobre a concessão de acesso.

Para verificar se essas decisões estão alinhadas com uma política, deve estar claro para cada usuário quais foram os motivos para a concessão do acesso e, subsequentemente, esses motivos devem ser checados visando o cumprimento da política de acesso da organização.

4.3 Controle de Acesso Mandatório (MAC)

As permissões são derivadas de uma política. Donos e usuários somente podem permitir acesso a outros dentro dos limites do que é declarado na política. Normalmente, essa política é gerenciada de forma centralizada. Uma política de MAC contém descrições de sujeitos, como pessoas, sistemas ou aplicações, e objetos como informações juntamente com outras aplicações ou sistemas.

O MAC usa atributos como credenciais e sigilo que estão ligados a sujeitos e objetos. Em um sistema baseado em MAC, o acesso é concedido ou negado avaliando se os atributos do sujeito que solicita o acesso correspondem aos requisitos de um objeto. Em um sistema baseado em MAC, os usuários individuais não são capazes de passar por cima das políticas de segurança, como é o caso de um ambiente DAC. Normalmente, as políticas de MAC para um sistema de informação são mantidas por um administrador do sistema.

A política de MAC diria que um usuário ou dono de dados pode acessar um diretório se ele estiver trabalhando no projeto relacionado. Não é possível que este usuário altere essa política sem o suporte de um administrador de sistema. Dentro de um ambiente MAC, um membro do projeto não será capaz de fornecer a alguém que não é membro o acesso ao diretório do projeto.

4.4 Controle de Acesso Baseado na Função (RBAC)

A principal diferença é que as autorizações não são baseadas em uma avaliação entre atributos. Aqui, as decisões de acesso se baseiam na função dos sujeitos, normalmente pessoas. Um dos motivos para introduzir RBAC é que, dentro de uma organização, há mais usuários do que funções. Visto que a gestão de todas as autorizações para cada usuário custa dinheiro, é possível poupar dinheiro quando podemos reduzir o número de usuários ou autorizações. O RBAC limita a variação do número de autorizações diferentes dentro de um sistema.

4.5 Controle de Acesso em Reivindicações (CBAC)

É uma forma relativamente nova e mais flexível de controle de acesso. No CBAC, o proprietário da informação ou um sistema define um conjunto de reivindicações necessárias antes de conceder o acesso. Um exemplo de tal afirmação é “o usuário trabalha para a organização X”. A vantagem do CBAC é que ele é mais flexível, uma vez que não se limita a reivindicações relacionadas a um papel.

4.6 Guardas de segurança em pontos de acesso

Além do controle de acesso, é importante monitorar quem tem acesso ao quê, e quando há abuso dessa autorização. Essa proteção do acesso a certas áreas lógicas pode ser por diversas razões, como restringir os riscos de roubo de identidade ou roubo de dinheiro, bem como cumprir determinados requisitos legais, tais como regulamentos de privacidade. Pode ser necessário demonstrar que a concessão de acesso não é apenas uma questão técnica, mas também uma preocupação organizacional.