IBM Security

IBM

Para uma melhor governança de acesso, analise os direitos além das funções

Com o IBM Security Identity Governance and Intelligence, você pode melhorar o controle de acesso ao integrar seus sistemas existentes, sem compromisso

Conheça nosso site

Fale com especialista

Por que as funções existem e por que elas não são mais suficientes

Há pouco tempo, as funções de trabalho eram relativamente fáceis de definir e controlar. Uma pessoa era um "contador", um "designer gráfico" ou um "parceiro de negócios". Mas, conforme as organizações crescem e os softwares de negócios se tornam mais sofisticados, novas funções foram adicionadas. "Contador, Nova York" pode exigir acesso diferente a aplicativos e dados do que "Contador, Chicago", por exemplo.

As funções foram criadas para facilitar o provisionamento e o desprovisionamento de usuários. E elas funcionavam. Ainda funcionam. A capacidade de fornecer a um novo usuário todo (ou grande parte) o acesso necessário para executar uma função de trabalho é muito mais rápida do que o provisionamento manual de usuários individuais para suas tarefas específicas em uma base ad-hoc.

O desafio vem da recente explosão nos números e tipos de funções de negócios. As organizações se tornaram tão focadas em ter a função perfeita para cada grupo de usuários que mesmo pequenas variações no perfil ou nas necessidades de acesso de uma pessoa levariam à criação de uma função totalmente separada. O problema foi: Se as restrições habilitadas pela TI que controlavam os direitos dos usuários (as permissões concedidas a eles) estivessem vinculadas somente a cargos gerais, as funções mais especializadas poderiam passar despercebidas, sem nenhum controle.

Com a governança de identidades, uma fabricante multinacional gerencia

430 milhões

de possíveis conflitos de direitos com o uso de algumas centenas de políticas.

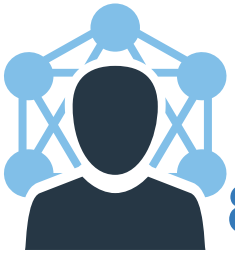
É importante proporcionar o alinhamento das necessidades e dos direitos de acesso

A criação de funções e a implantação de ferramentas de gerenciamento de identidade permitiram que as organizações compreendessem quais usuários tinham acesso a quais aplicativos, além de quando o acesso era concedido a esses usuários.

Mas essa informação básica não é mais suficiente para proporcionar segurança e controle. As organizações também precisam saber se os usuários com acesso têm o acesso ***certo***. Mais importante, elas precisam garantir que os usuários não tenham o acesso ***errado***.

A grande quantidade de funções específicas implica no aumento de funções não somente em quantidade, mas também em complexidade. E as funções estão em constante mudança. Dessa forma, as funções não são mais a ferramenta certa para controlar as identidades dos usuários. As organizações precisam analisar mais detalhadamente quem tem quais direitos e como eles são usados.

Uma maneira importante e eficaz de obter as percepções necessárias sobre os usuários e seus direitos é pensar como um auditor. Isso pode ajudar a reduzir os problemas, garantindo a implementação dos controles necessários para evitar violações. Roberto não usou um determinado direito nos últimos 6 meses? Isso geralmente é um bom motivo para revogar o privilégio. Vanessa tem a capacidade de iniciar uma solicitação, por exemplo, para a compra de um equipamento, e depois aprovar seu próprio pedido? Outro motivo para revogar.



Com a IBM, um e-commerce global remove quase

80% dos privilégios de acesso do usuário

após a descoberta de acesso não frequente.

Pensar como um auditor aborda adequadamente as necessidades de negócios e de TI

Uma solução de governança de identidades fácil de auditar é essencial para o gerenciamento eficiente de usuários e seus direitos. Os auditores dão grande importância em ter as regras certas para identificar as violações de segregação de tarefas. Eles também exigem controles para remover e evitar essas violações.

Mas tem mais. Para ser mais eficiente, é necessário não apenas pensar como um auditor, mas também falar como um. A linguagem mais usada na governança de identidades usa a terminologia dos mundos de TI e de negócios. Porém, essa combinação pode ser um problema para os auditores que não entendem a linguagem de TI e preferem usar termos de negócios. A solução certa de governança de identidades reúne os mundos de negócios e TI para ajudar as organizações a entender se os usuários têm ou não acesso aos aplicativos apropriados e para oferecer suporte a decisões de negócios e ações que dependem do acesso apropriado.

IBM® Security Identity Governance and Intelligence oferece a capacidade de ver além das funções para uma visão detalhada dos direitos e atividades de negócios. A solução IBM oferece a inteligência necessária para revogar, reatribuir ou adicionar direitos com precisão e eficácia, ajudando você a atender às necessidades de negócios sem comprometer a segurança.

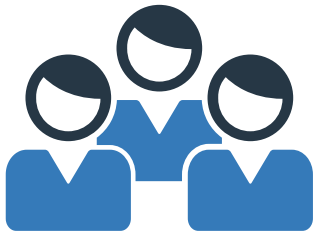
Um banco na França reduz seu catálogo de direitos, mostrando aos usuários de 10-15 itens em vez de centenas.

Por que as atividades de negócios são uma base melhor para a governança

Pense em uma função como uma coleção de direitos. É uma maneira de definir os tipos de acesso necessários para as pessoas que realizam tarefas iguais ou semelhantes. Esses direitos podem variar de acesso a software de e-mail (concedido a todos), acesso a um aplicativo que gerencia uma propriedade intelectual (concedido a poucos) e acesso a funções muito específicas do aplicativo (com acesso mais limitado).

É um processo de diversas fases: Um funcionário recebe uma função (por exemplo, corretor de valores). Essa função vem com direitos que permitem o acesso a recursos de software (como inserir um pedido de comercialização). Esse recurso permite uma atividade de negócios específica (posicionamento de comercialização). Mas o corretor de valores está impedido de aprovar a mesma comercialização. Esse direito é concedido somente a pessoas que não têm permissão para realizar um posicionamento de comercialização. As tarefas são segregadas para evitar conflitos.

O problema com as funções é que elas evoluem constantemente. Dentro de cada função, pode haver diversas outras funções ou funções aninhadas, o que pode gerar confusão, violações no compliance e vulnerabilidades de segurança. Porém, um auditor que está criando ou aplicando uma regra pode não entender muito bem as funções. Sabe qual é o resultado? Podem ocorrer algumas violações de segregação de tarefas.



Uma empresa europeia de seguros e finanças controla o acesso de

75.000 usuários

de aplicativos SAP, distribuídos e de mainframe.

Veja como a abordagem baseada em atividades de negócios funciona

O que aconteceria se você segregasse as tarefas de duas funções, "web design" e "folha de pagamento", para impedir a publicação de salários de funcionários no site da empresa? Mas imagine que uma pessoa da equipe de folha de pagamento também tenha trabalhado em projetos paralelos, o que ofereceu a ela a capacidade de publicar no site sem ter a função "web design". Para evitar esse cenário, todas as possíveis combinações de funções (e subfunções) das funções de web design e folha de pagamento precisariam ser gerenciadas, uma tarefa praticamente impossível sem as ferramentas de governança de identidades apropriadas e automatizadas.

Em vez de controlar identidades e segregar o acesso com o conceito abstrato de funções, por que não usar algo mais simples? É aí que entra a governança com base nas atividades de negócios. Em vez de usar funções intituladas como "web design" e "folha de pagamento", use uma linguagem simples para descrever atividades, como "capacidade de editar o site" e "capacidade de ver informações sobre a folha de pagamento".

Nessa abordagem, a organização e o auditor sabem exatamente quais recursos cada usuário possui. Além disso, subcategorias de atividades (como "editar gráficos em um site") são automaticamente consideradas parte de uma categoria maior (como "editar um site"), portanto, não há necessidade de gerenciamento manual, como acontece ao usar funções. Em muitos casos, um auditor não entenderá quais funções específicas podem e não podem se sobrepor sem conflito. Porém, os auditores entenderão quais ***atividades de negócios***, quando usadas em conjunto, poderão apresentar uma violação de segregação de tarefas e um risco de segurança.

A solução certa de governança de identidades ajuda você a controlar o acesso de seus usuários a atividades de negócios com visibilidade consolidada e detalhada dos direitos, não somente das funções. As funções mudam, se sobrepõem e aumentam. Dessa forma, o acesso deve ser controlado no nível dos direitos, permitindo uma visão dos recursos específicos que o usuário possui, em vez de depender dos grupos confusos de acesso concedido a uma função. A solução certa pode fornecer a inteligência necessária para que você tome as decisões apropriadas sobre quem tem e quem deve ter acesso ao quê.

Em resumo: Controlando com soluções inteligentes IBM

O IBM Security Identity Governance and Intelligence cria condições para aprimorar os negócios ao permitir a concessão dos direitos certos às pessoas certas. Usando sua visibilidade completa dos direitos, é possível aplicar melhor as políticas de segregação de tarefas para garantir que os usuários atualmente autorizados não tenham direitos conflitantes. Você pode gerenciar contas órfãs para garantir que os usuários antigos não continuem com acesso após saírem da organização. Também é possível automatizar controles e relatórios. A abordagem da IBM permite controlar o uso de atividades de negócios, destacando funções complexas para facilitar o gerenciamento para os auditores e simplificar as tarefas de governança.

O IBM Security Identity Governance and Intelligence conecta os pontos de vista de TI, compliance e negócios para reduzir os riscos de acesso. Ao consolidar direitos de acesso refinados de aplicativos corporativos em um repositório central e estruturá-los em funções de negócios, por exemplo, ele oferece melhor visibilidade do acesso real do usuário.

Como parte integral do compromisso da IBM com a liderança em gerenciamento de identidade e acesso, o IBM Security Identity Governance and Intelligence desempenha uma função importante no portfólio de segurança de TI da IBM. As soluções IBM, incluindo recursos de segurança abrangentes e percepções fornecidas pela pesquisa e desenvolvimento do IBM X-Force®, foram projetadas para ajudar a proteger aplicativos e dados essenciais aos negócios contra ameaças de segurança, incluindo possíveis conflitos por falhas nos controles.

E.ON Global Commodities precisava impedir

a comercialização não autorizada.

Com a IBM, ela melhorou:

- **o gerenciamento da segregação de tarefas**
- **o fornecimento de relatórios aos auditores**
- **o entendimento do fluxo de informações na empresa**

Assista ao vídeo introdutório E.ON da IBM.

Para obter mais informações

Para saber mais sobre o IBM Security Identity Governance and Intelligence, fale com o nosso especialista de segurança da IBM, ou acesse: **https://www.ibm.com**/security/br-pt

Sobre as soluções IBM Security

O IBM Security oferece um dos portfólios mais avançados e integrados de produtos e serviços de segurança corporativa. O portfólio, com suporte de pesquisa e desenvolvimento X-Force mundialmente conhecidos, fornece inteligência de segurança para ajudar as organizações a proteger holisticamente pessoas, infraestruturas, dados e aplicativos, oferecendo soluções para gerenciamento de identidade e acesso, segurança de banco de dados, desenvolvimento de aplicativos, gerenciamento de riscos, gerenciamento de terminal, segurança de rede e muito mais. Essas soluções permitem que as organizações gerenciem os riscos de maneira eficiente, além de implementar a segurança integrada para arquiteturas de negócios, móveis, em nuvem, de mídia social, entre outras. A IBM opera uma das organizações de pesquisa, desenvolvimento e entrega de segurança mais amplas do mundo, monitora 15 bilhões de eventos de segurança por dia em mais de 130 países e detém mais de 3.000 patentes de segurança.

Além disso, o IBM Global Financing oferece inúmeras opções de pagamento para ajudá-lo a adquirir a tecnologia necessária para permitir o crescimento dos seus negócios. Oferecemos gerenciamento completo do ciclo de vida de produtos e serviços de TI, desde a aquisição até a distribuição. Para obter mais informações, acesse: **http://ibm.com**/financing/br-pt

Conheça nosso site

Fale com especialista

IBM Security
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América
Outubro de 2016

WGW03177-BRPT-00