TORNANDO TUDO MAIS FÁCIL

Edição Especial da SailPoint

Segurança de Identidade Moderna

para leigos®
A Wiley Brand

Veja por que a identidade é o novo perímetro de segurança

Descubra como a segurança de identidade gera valor de negócios

Empregue IA para automatizar a segurança de identidade

Oferecido pela

SailPoint

Steve Kaelble

Sobre a SailPoint

A SailPoint equipa a empresa moderna a gerenciar e proteger com facilidade o acesso a aplicativos e dados do ponto de vista da identidade, na velocidade e escala necessárias. Como líderes da categoria, reinventamos continuamente a segurança da identidade como a base da empresa segura. A SailPoint oferece uma plataforma unificada, inteligente e extensível, que foi criada para servir de defesa contra as atuais ameaças cibernéticas dinâmicas e centradas na identidade, aumentando a produtividade e a eficiência. A SailPoint ajuda muitas das empresas mais complexas e avançadas do mundo a criar um ecossistema de tecnologia seguro que promove a transformação dos negócios.

Segurança de Identidade Moderna

Edição Especial da SailPoint

Steve Kaelble

para leigos®
A Wiley Brand

Segurança de Identidade Moderna para Leigos®, Edição Especial da SailPoint

Publicado por
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774, Estados Unidos
www.wiley.com

ISBN 978-1-394-37893-7 (pbk); ISBN 978-1-394-37894-4 (ePDF);
ISBN 978-1-394-37895-1 (ePub)

Créditos da editora

Editora: Elizabeth Kuball
Editora de aquisições: Traci Martin
Editor gerente sênior: Rev Mengle
Gerente de contas de clientes: Jeremith Coward
Editor de produção: Umeshkumar Rajasekhar

NESTE CAPÍTULO

- O que é segurança de identidade
- Resolvendo equívocos de segurança de identidade
- Entendendo a importância da segurança de identidade
- Principais benefícios

Capítulo 1
O que é segurança de identidade moderna

As tecnologias digitais movem o mundo e as identidades digitais acessam continuamente essas tecnologias. Este capítulo mostra como a segurança de identidade ajuda as empresas a controlar e a monitorar com segurança o acesso a tecnologias digitais, mesmo quando as arquiteturas de nuvem e a inteligência artificial adicionam complexidades.

Definindo a segurança de identidade

Pouco tempo atrás, a segurança de identidade era, de um modo geral, um tópico de interesse principalmente para pessoas de tecnologia da informação (TI). Em seguida, as histórias de horror começaram a tomar conta das manchetes, e todos na empresa, dos menos graduados até a diretoria, perceberam que as violações podem ser desde uma ameaça operacional até uma ameaça existencial. À medida que os cenários de TI tornaram-se mais complexos, o mesmo aconteceu com a tarefa de protegê-los contra as ameaças cibernéticas e garantir a conformidade com regulamentos de privacidade mais amplos.

LEMBRE-SE

Perdido em meio a toda essa complexidade existe um fato surpreendentemente simples: a segurança empresarial é realmente uma questão de identidade. É uma questão de verificar e conhecer a identidade de cada pessoa e entidade que pode acessar recursos digitais e dados críticos e, em seguida, garantir que apenas as identidades certas tenham acesso apenas a exatamente aquilo a que precisam ter acesso.

LEMBRE-SE

Com isso em mente, o ponto-chave ao atuar com segurança no mundo digital de hoje é o conceito de *segurança de identidade*. Às vezes, a segurança de identidade é chamada de *governança e administração de identidade* (identity governance and administration, IGA); no entanto, a segurança de identidade é muito mais do que isso. A segurança de identidade vai além da IGA tradicional porque combina governança de acesso dinâmico, insights orientados por IA, aplicação de políticas e avaliação contínua de riscos. É assim que a empresa fornece tecnologia vital a uma força de trabalho diversificada e, ao mesmo tempo, se protege contra as inevitáveis ameaças cibernéticas.

Aqui estão alguns conceitos associados à segurança de identidade:

- **Gerenciamento de identidade e acesso (Identity and access management, IAM).** Essa especialidade automatiza a atribuição e a revisão de acesso, para que apenas as pessoas certas tenham acesso rigorosamente dosado apenas aos dados e aplicativos certos, nos momentos certos, pelos motivos certos.
- **Gerenciamento de acesso privilegiado (privileged access management, PAM).** Esse subconjunto do IAM concentra-se em proteger as contas privilegiadas dos usuários cujo trabalho exige que eles acessem bancos de dados, sistemas de back-end e outros locais confidenciais.
- **Gerenciamento de acesso (access management, AM).** Esse conceito refere-se à autenticação por meio da concessão de várias identidades de acesso a aplicativos por meio de tecnologias como logon único (SSO) e autenticação multifator (MFA).

A segurança de identidade amplia esses conceitos para que as organizações possam melhorar e automatizar seus processos a fim de validar o acesso com privilégios mínimos, garantir que o acesso seja revisado adequadamente e assegurar a existência de políticas de separação de tarefas em vigor e a sua aplicação. O mais importante é a responsabilidade, a transparência e a mitigação de riscos.

Resolvendo equívocos de identidade

Conforme descrito na seção anterior, a segurança de identidade abrange vários conceitos relacionados. Imagine isso como algo maior do que a soma de suas partes, porque qualquer um desses conceitos por si só não faz todo o trabalho de forma efetiva ou eficiente.

Por exemplo, a segurança de identidade pode soar como gerenciamento de acesso, à medida que incorpora serviços como SSO e MFA. Esses serviços de três letras são essenciais para a segurança de identidade,

particularmente a tarefa de autenticar a identidade de uma pessoa ou entidade que busca acesso.

LEMBRE-SE

No entanto, a autenticação é apenas o primeiro passo. Imagine um cartão de embarque de uma empresa aérea. Basta mostrá-lo no portão de embarque junto com sua carteira de identidade ou passaporte válido e você estará autenticado como passageiro. A próxima pergunta é: onde você está autorizado a se sentar? Primeira classe ou econômica? Em que grupo de embarque você está? Você tem direito a uma refeição gratuita? O seu cartão de embarque fornece a devida autorização?

No contexto da segurança de identidade, a autorização é o processo de verificação do que um usuário autenticado tem permissão para acessar: que aplicativos, arquivos e dados específicos. A autenticação acontece primeiro, com a ajuda de verificadores como senhas, números de identificação pessoal (PINs), biometria e perguntas de segurança. Em seguida, vem a autorização, com base nas configurações e políticas estabelecidas pela organização. Estes são dois métodos comuns de autorização:

- **Controle de acesso baseado em função (role-based access control, RBAC).** O acesso é determinado pela função do usuário na organização. O RBAC ajuda as pessoas em funções específicas a obter o acesso de que precisam para realizar o seu trabalho de modo bem-sucedido, mas nada além do que sua função precisa.
- **Controle de acesso baseado em atributos (attribute-based access control, ABAC).** Esse controle é mais granular do que o RBAC e adiciona atributos específicos do usuário, como nome, ID e credenciamento de segurança. Os atributos do ABAC também podem incluir o tempo de acesso, a localização dos dados e o nível atual de ameaça organizacional.

Reconhecendo por que a segurança de identidade é vital

Os ataques cibernéticos e as ameaças baseadas em identidade estão cada vez mais disseminados, com um impacto cada vez maior nas organizações. Os impactos nos negócios incluem perda de receita, danos à reputação e custos de contenção. Esses impactos cada vez piores tornam a segurança de identidade cada vez mais crítica.

DICA

Os requisitos de conformidade também são uma preocupação cada vez maior; as organizações precisam de toda a ajuda possível, não apenas para atender às necessidades de conformidade, mas também para comprovar a conformidade de maneiras auditáveis. As ferramentas de segurança de identidade são incrivelmente úteis para isso.

LEMBRE-SE

Em última análise, a segurança de identidade é essencial para garantir a segurança e a conformidade. Além disso, ela abre as portas para uma maior produtividade dos negócios que geram crescimento. A tecnologia é capaz de levar ao sucesso dos negócios apenas se ela for acessível às pessoas que precisam usá-la e a segurança de identidade facilita esse acesso, mantendo afastados aqueles que não devem ter acesso.

Benefícios da segurança de identidade moderna

Quais são os fatores mais importantes da segurança de identidade? Uma pista já está no nome: segurança. Esse é um fator de peso, mas está longe de ser o único. Aqui estão alguns dos principais benefícios:

- **Redução dos custos operacionais.** Um programa de segurança de identidade sólido automatiza os processos de governança e administração de identidade que exigem muita mão de obra. Certificações, solicitações de acesso, gerenciamento de senhas e provisionamento: tudo isso pode ser automatizado para reduzir de maneira drástica os custos operacionais. Os usuários têm opções de autoatendimento para lidar com suas próprias necessidades, reduzindo a duração de algumas tarefas de acesso de horas para minutos. A equipe de TI pode reduzir os custos em até 15%, dedicando menos tempo a tarefas administrativas e mais tempo agregando valor de outras maneiras.
- **Melhor conformidade e desempenho de auditoria.** Uma forte segurança de identidade ajuda a verificar se estão sendo usados os controles certos para garantir a conformidade com uma série de regulamentos de segurança e privacidade, como a lei Health Insurance Portability and Accountability Act (HIPAA), o General Data Protection Regulation (GDPR) e a lei Sarbanes–Oxley Act (SOX), para citar apenas alguns de maior destaque. As auditorias e a conformidade são muito menos complicadas quando as ferramentas certas estão disponíveis.
- **Maior eficiência.** De forma geral, é muito melhor quando os usuários têm acesso fácil aos aplicativos e dados de que precisam para realizar suas funções com sucesso. Eles ficam mais produtivos, de forma mais rápida, mesmo quando mudam de função.
- **Redução de riscos e maior segurança.** Sim, dissemos que a segurança era uma das razões. A segurança de identidade oferece uma visão centralizada de quem tem acesso a quê. Com a ajuda da automação, a segurança de identidade detecta rapidamente acessos inadequados, controles fracos ou violações de políticas e, em seguida, lida com isso e corrige os problemas.

NESTE CAPÍTULO

- O que é o gerenciamento do ciclo de vida da identidade
- Provisionamento de acesso aos usuários
- Configuração de políticas e controles

Capítulo 2
Criando um programa de segurança de identidade

O que é necessário para criar um programa moderno de segurança de identidade? Tudo começa com uma imagem completa do ciclo de vida de uma identidade, que inclui a criação, a evolução e, quando chega a hora, o término. Trata-se de conceder acesso, estabelecer políticas e controles, garantindo que todo o trabalho atenda às necessidades não apenas de segurança, mas de outras exigências de conformidade corporativa. Este capítulo contém os detalhes específicos.

Gerenciando o ciclo de vida

Imagine as identidades digitais como se fossem seres vivos. Isso pode parecer um pensamento típico de ficção científica, mas as identidades possuem ciclos de vida. Eles têm um início, evoluem, suas necessidades mudam e, posteriormente, a vida delas termina. O gerenciamento desse ciclo de vida é um componente essencial de um programa de segurança de identidade. Além disso, é um componente que pode ser um trabalho manual árduo e demorado ou um processo eficiente e amplamente automatizado ou até mesmo de autoatendimento.

DICA

Um programa moderno e unificado de segurança de identidade automatiza o gerenciamento e o controle do que, de outra forma, seriam desafios complexos. Uma estratégia voltada para o ciclo de vida pode fazer maravilhas para o provisionamento e o desprovisionamento automatizados sempre que alguém entra em uma empresa, muda de cargo, ou a deixa.

É um método que capacita os usuários empresariais a solicitar e gerenciar o acesso a recursos, sem ocupar a equipe de TI. Esse método deve

fornecer visibilidade e controle de acesso, seja para funcionários, terceirizados ou até mesmo usuários não humanos, como bots, contas de serviço e assim por diante. Ele deve ser capaz de evoluir, alterando adequadamente o acesso à medida que a função do usuário muda. Além disso, a equipe de conformidade deve ter a capacidade de obter facilmente as informações de que precisa ao responder a auditorias.

Veja como um sistema moderno lida com o provisionamento automatizado:

- A criação de contas e o acesso a aplicativos e dados são automatizados.
- A concessão de acesso e direitos iniciais é precisa e baseada em dados.
- O sistema reconhece novos usuários e sabe quando eles mudam de cargos ou deixam a empresa.
- Adota-se um modelo de acesso de privilégios mínimos, com visibilidade de qualquer superprovisionamento ou contas órfãs.

E veja como as solicitações de acesso são tratadas:

- Os usuários podem fazer uma solicitação de novo acesso, para si ou para terceiros, a partir de um catálogo de funções e direitos que é criado e atualizado automaticamente.
- A inteligência artificial (IA) generativa ajuda a criar descrições de direitos fáceis de entender para informar os aprovadores que devem determinar se essa solicitação é apropriada.
- Recomendações orientadas por IA com base nas atividades ajudam a informar as determinações sobre qual acesso deve ser concedido.
- O sistema identifica a justificativa para solicitações de acesso, o que contribui para decisões mais adequadas e fornece uma trilha de auditoria.
- É fácil conceder acesso temporário e com prazo definido.
- Uma interface mostra o andamento das solicitações de aprovação.

Provisionando os usuários

LEMBRE-SE

Uma etapa fundamental na segurança de identidade é o *provisionamento de usuários*, que é o processo de criação da identidade digital e dos privilégios de acesso de um usuário para vários recursos que podem ser locais, em nuvem ou em um ambiente híbrido. O provisionamento de usuários leva em consideração o nome, a função, o departamento de

uma pessoa, além de vários atributos, direitos, associações, além de outros dados.

Alguns aspectos do provisionamento de usuários são de autoatendimento, ao passo que outras etapas podem ser discricionárias, incluindo o acesso a dados e aplicativos. Após a obtenção das autorizações obrigatórias, o acesso em alguns casos pode ser concedido com base nos requisitos de fluxo de trabalho. E o ideal é que grande parte do processo seja automatizado e tratado por um software que aplique as regras estabelecidas.


DICA

O provisionamento deve mudar à medida que as funções do usuário e as necessidades de negócios mudam. Quando um funcionário passa de uma função para outra, ou assume uma atribuição temporária, parte desse acesso precisa ser removida, ao passo que o acesso a outros recursos precisa ser adicionado.

O oposto do provisionamento é o *desprovisionamento*, que é a revogação do acesso e dos privilégios com base nas alterações de função ou quando um funcionário deixa a empresa. O desprovisionamento é extremamente importante, porque ainda que um funcionário exemplar deixe a empresa nas melhores circunstâncias, se a sua conta ficar inativa, ela poderá se tornar uma porta de entrada para ataques cibernéticos.

As práticas recomendadas no provisionamento de usuários incluem políticas e processos centralizados de segurança de identidade. É fundamental automatizar o processo, pois isso reduz o risco de provisionamento acima ou abaixo do nível necessário que pode acontecer com sistemas manuais. O princípio do privilégio mínimo deve ser adotado como referência para uma solução moderna de segurança de identidade, pois garante que os usuários obtenham apenas o acesso de que precisam para fazer seu trabalho. A autenticação baseada em risco pode bloquear automaticamente os usuários se forem detectadas ações problemáticas.


LEMBRE-SE

A auditoria e os relatórios também são elementos essenciais, porque as preocupações com a segurança geralmente coincidem com os requisitos de conformidade. A auditoria interna e os relatórios são ideias proativas que apoiam as iniciativas de conformidade e a melhor postura de segurança. O programa de segurança de identidade certo pode documentar controles de mitigação de risco e coordenar uma série de atividades de conformidade que lidam bem com deficiências e violações de auditoria. A próxima seção aborda esse assunto em mais detalhes.

Estabelecendo controles de acesso

No contexto da segurança de identidade, não são apenas as pessoas que têm identidades. Dispositivos conectados e IA também podem ter identidades, apenas para citar algumas possibilidades. Com a complexidade

cada vez maior dos ambientes de várias nuvens, vários tipos de recursos de nuvem devem interagir constantemente. A segurança de identidade moderna e unificada deve se estender à infraestrutura de nuvem e às identidades de nuvem.

LEMBRE-SE

É onde a *gestão de direitos* se torna vital. A segurança de identidade inclui a definição dos direitos atribuídos a sistemas, aplicativos, dados e serviços de nuvem — as permissões e limites que declaram o que eles têm acesso e quais ações podem tomar. Dada a natureza em constante mudança dos ambientes de nuvem, o gerenciamento de direitos precisa de visibilidade e controle refinados, com ajuste automático e detecção de direitos excessivos. Como sempre, o objetivo é o privilégio mínimo.

O *controle de acesso baseado em função* (role-based access control, RBAC) torna o provisionamento mais simples, conectando identidades com funções definidas na empresa. Se uma pessoa for aprovada para uma função ou tarefa, serão concedidas permissões e direitos de acesso específicos automaticamente. Se essa pessoa deixar essa função, o acesso será ajustado ou removido automaticamente.

O *controle de acesso baseado em política* (policy-based access control, PBAC) ou *controle de acesso baseado em atributo* (attribute-based access control, ABAC) aplica políticas com base em características como departamento, local, gerente e até mesmo atributos, como a hora do dia, o comportamento normal da identidade, os relacionamentos com terceiros e as ações solicitadas. É possível obter atributos de uma variedade de fontes de dados, não apenas ferramentas de identidade, mas também aplicativos de recursos humanos e sistemas de planejamento de recursos empresariais (ERP). Isso permite uma estratégia granular de acesso.

Outro conceito importante a ser incorporado às estratégias de segurança de identidade é a *separação de funções* (às vezes chamada de *segregação de funções*, ou SoD, separation/segregation of duties). Segundo esse princípio, nenhum usuário deve ter controle total sobre certos tipos de atividades, processos ou sistemas sensíveis. A conclusão de um processo confidencial deve exigir o envolvimento de mais de uma pessoa.

Por exemplo, a pessoa que autoriza os pagamentos por cheque não deve ser a mesma pessoa que assina o cheque eletronicamente. Esse tipo de regra rígida é conhecida como *imposição estática*. *Imposição dinâmica* significa que os controles são determinados em tempo real, portanto os usuários precisam obter aprovação de outra pessoa autorizada para executar uma tarefa.

A SoD é uma boa prática por muitos motivos, entre eles, evitar possíveis problemas de contabilidade e segurança cibernética. É por isso que a SoD é, na realidade, um requisito de conformidade, chegando a ser uma disposição da lei Sarbanes–Oxley (SOX).

NESTE CAPÍTULO

- Uso da IA para potencializar os processos de identidade
- Emprego da IA para detectar ameaças
- Automatização com a ajuda da IA

Capítulo 3
Utilizando a IA e a automação

Inteligência artificial está chegando a todos os tipos de trabalho em todos os tipos de empresas, fornecendo resultados poderosos e eliminando tarefas rotineiras. Não é de surpreender que a segurança de identidade orientada por IA seja a chave para o controle automatizado e centralizado sobre o acesso a dados, aplicativos, sistemas e infraestrutura de nuvem, além de fornecer visibilidade de 360 graus quanto ao risco. Este capítulo mostra como a IA potencializa a segurança de identidade.

Simplificando os processos de identidade

A inteligência de dados orientada por IA pode automatizar a descoberta, o gerenciamento e o controle do acesso dos usuários. Isso torna o processo de discernimento de acesso mais rápido e confiável, além de facilitar a detecção e a resposta a possíveis ameaças.


DICA

Para os gerentes de negócios, as equipes de identidade e os proprietários de aplicativos, a IA ajuda a criar e otimizar um modelo de acesso sempre adaptável. Os dados de identidade que você já possui se transformam em insights capazes de modelar o acesso correto para cada identidade e apoiar a tomada de decisão. Além disso, por lidar com as tarefas repetitivas, a IA permite um maior foco no acesso de alto risco.

A IA ajuda os profissionais de gestão de riscos a serem mais proativos em detectar acessos de risco e tomar as devidas providências. Isso dá

aos profissionais de segurança de identidade visibilidade abrangente de que precisam para garantir a conformidade. E para os usuários finais, ela fornece o acesso de que precisam para que sejam o mais produtivos possível desde o primeiro dia, adaptando-se às mudanças constantes e, ao mesmo tempo, garantindo o mínimo de privilégios.

DICA

Se analisarmos o trabalho de escrever descrições para direitos, por exemplo. Essas descrições são essenciais, mas podem ser uma tarefa repetitiva e demorada de realizar. Como mostra o SailPoint Identity Security Cloud, a IA generativa pode ajudar. As descrições criadas automaticamente podem melhorar as revisões de acesso e são úteis em governança e conformidade.

A IA também pode ser um divisor de águas no emprego de controle de acesso baseado em função (RBAC). No passado, o design de funções dependia de um esforço manual e demorado. Com um programa moderno de segurança de identidade, a IA pode assumir essa tarefa. A IA pode analisar vários usuários, dividi-los em grupos por categoria e, em seguida, identificar proativamente quem tem acesso atípico. A IA pode criar funções de modo automático, identificando clusters de acesso semelhante e, em seguida, atribuindo o nível certo de acesso necessário para cada função definida. Ela pode então identificar usuários com acesso atípico e corrigir o risco de acesso desses usuários.

Durante o processo, a IA cria um modelo de acesso que maximiza a produtividade com o mínimo de privilégio. A partir daí, ela usa a análise e as recomendações de funções contínuas alimentadas por aprendizado de máquina (machine learning, ML) para manter o modelo, usando análises automáticas para descobrir funções novas e especializadas. Tudo feito de forma a minimizar o envolvimento administrativo.

O modelo de acesso também é essencial para reforçar a segurança além das equipes de trabalho empregadas. O gerenciamento do ciclo de vida de todas as identidades, mas especialmente de não funcionários e máquinas, pode ser difícil e demorado. Por isso, é perfeito para se beneficiar de um sistema centralizado e orientado por IA.

DICA

A solução SailPoint ajuda as organizações a rastrear e controlar com eficiência o acesso de máquinas e pessoas que não são funcionários em tempo integral, como terceirizados, fornecedores ou parceiros de negócios. A solução agiliza a colaboração entre equipes internas e externas para coletar e gerenciar detalhes de identidade, garantindo que as pessoas certas tenham o acesso certo quando precisarem — e que o acesso seja removido quando não precisarem. Essa prática reduz os riscos de segurança, melhora a conformidade e torna o gerenciamento de identidades de não funcionários mais rápido e fácil.

O caminho para a segurança de identidade moderna e unificada também envolve a integração de aplicativos que podem contar com a governança de um sistema. Normalmente, dois tipos de aplicativos são compatíveis. Os aplicativos de acesso, aqueles que fornecem contexto para direitos de acesso, solicitações e políticas de acesso. Os aplicativos corporativos, que precisam de funções de segurança de identidade para gerenciar o acesso às contas existentes neles. Eles podem ser plataformas locais ou de software como serviço (SaaS).


DICA

A integração de aplicativos revela aplicativos corporativos que podem ser adicionados ao programa de segurança de identidade. Isso ajuda a agilizar, reduzindo o tempo necessário para o processo de integração e configuração desses aplicativos. Essa prática garante que os aplicativos estejam sujeitos a toda a gama de recursos de segurança de identidade, acelerando o tempo de retorno sobre o investimento para uma organização.

Detectando ameaças

"Encontrar uma agulha no palheiro." O provérbio compara-se à tarefa de detectar um comportamento atípico, ou seja, quase impossível de se encontrar. O mesmo princípio vale para os comportamentos atípicos de identidade. No entanto, identificá-los é fundamental para proteger um ambiente moderno e orientado por dados.


DICA

Essa é outra área em que a inteligência artificial e o aprendizado de máquina podem ser úteis. Os dois são tecnologias incrivelmente poderosas para procurar no palheiro de identidades e ver quem se destaca com padrões que se desviam da norma.

Nem todos os comportamentos atípicos são nocivos, é claro. Um comportamento atípico de identidade pode ser um usuário privilegiado com níveis de acesso mais altos do que a maioria, uma conta de sistema que está lidando com tarefas automatizadas ou alguém que assumiu uma tarefa de curto prazo com diferentes necessidades de acesso. Mas, às vezes, um comportamento atípico é uma conta comprometida ou uma ameaça interna, e as duas podem ter se desviado do comportamento aceitável para a algo mal-intencionado.

As tecnologias de ML aprendem a partir de um vasto volume de dados de identidade e podem detectar até padrões sutis com incrível precisão. O ML consegue detectar combinações de acesso prejudiciais que podem facilitar o roubo de dados ou fraude. Ele também detecta ameaças muito rapidamente, o que minimiza a janela de oportunidade para os autores de ameaças.

LEMBRE-SE

Você precisa de um painel de comportamentos atípicos que ofereça uma perspectiva ampla do cenário desses comportamentos. Esse recurso atribui a cada comportamento atípico uma pontuação de risco, com limites de risco baseados na tolerância ao risco organizacional. Esta tarefa claramente está além do alcance das capacidades humanas. Identificar um comportamento atípico é uma tarefa complexa, com base em vários fatores, como o número de direitos, a singularidade da função, o acesso raro e as semelhanças/diferenças em comparação aos colegas.

Esse trabalho deve ser realizado constantemente, em tempo real. Se for detectada uma ameaça, o sistema deve revogar o acesso automaticamente. Uma variedade de táticas de remediação direta e indireta pode reduzir as ameaças de comportamentos atípicos. E é possível tomar uma decisão estratégica de ignorar um comportamento atípico com base em fatores únicos relacionados à identidade específica.

Adotando a IA agêntica para automatizar

Existem inúmeras maneiras de empregar a IA agêntica para automatizar o trabalho de segurança de identidade, além dos exemplos de IA citados anteriormente. Os provedores de soluções pesquisam continuamente tarefas repetitivas do cliente que podem ser deixadas a cargo de agentes inteligentes automatizados para assistência, orientação e interações em linguagem natural.

Minimizar a intervenção manual é um dos principais objetivos. O trabalho de segurança de identidade é essencial, mas também é vital para a empresa evitar que os requisitos de segurança se tornem um gargalo de produtividade. A IA simplifica os processos para conceder acesso apropriado rapidamente.

Conforme descrito anteriormente, a IA agêntica também pode realizar tarefas que os seres humanos simplesmente não podem fazer na escala necessária. Observar constantemente os valores atípicos de identidade e as ameaças de forma eficaz: é aqui que a IA é absolutamente essencial. Cada vez mais, o mesmo acontece com a criação e a adaptação contínua de modelos de acesso.

DICA

Simplificar os processos de identidade em um gerenciamento centralizado leva a uma governança de acesso mais forte, o que agrada à equipe de conformidade. Os insights orientados por IA ajudam a identificar acessos de risco e garantem que o acesso esteja correto e alinhado com os requisitos regulatórios e de segurança de identidade. Uma visão de 360 graus permite relatórios favoráveis aos negócios que satisfazem os reguladores. Comprovar a separação de funções é uma conquista a mais no cumprimento dos regulamentos.

NESTE CAPÍTULO

- Como evitar armadilhas comuns
- Criar um roteiro de segurança de identidade e implementá-lo

Capítulo 4
Dez dicas para melhorar a segurança de identidade

Você perde o sono pensando se as atuais práticas de segurança da sua empresa são efetivas? Quer elevar o nível de maturidade em segurança de identidade da sua organização? Leia as dez dicas para ajudar a melhorar a segurança de identidade no ambiente corporativo.

- **Abandonar o uso de senhas.** As senhas existem desde que existem contas seguras em computadores. Mas, na verdade, elas não podem garantir a segurança porque são vulneráveis a violações, mesmo que você inclua dados biométricos ou outros fatores extras. Em última análise, proteger um login não fornece proteção contra acesso definido de forma inadequada. A segurança de identidade é o perímetro que você deve construir e defender.
- **Adotar privilégios mínimos.** A melhor defesa é garantia de que nenhum usuário, físico ou não, possa ter acesso além do que é necessário para executar sua função corretamente. O conceito de privilégio mínimo minimiza os riscos, garantindo que os usuários tenham apenas as permissões absolutamente necessárias. Isso limita as superfícies de ataque, frustra as ameaças internas e aumenta a conformidade com as políticas e os regulamentos.
- **Pensar além da TI.** A segurança diz respeito a todos, não apenas às equipes de segurança de TI, mas também aos proprietários de aplicativos e inclusive aos executivos. A segurança de identidade protege contra ameaças que podem interromper as operações e causar terríveis danos financeiros e de reputação. Mas, quando feita corretamente, também viabiliza uma maior produtividade geral, facilitando não apenas a conformidade com a privacidade, mas também a conformidade com os regulamentos financeiros.

- **Definir uma visão.** A visão para o seu programa de segurança da identidade deve ter como base as tendências que moldam o futuro da segurança da identidade e a maturidade do seu programa hoje. Procure saber o que mais a sua organização também espera obter para os usuários finais, a equipe de TI, os especialistas em conformidade e os negócios em geral. A segurança da identidade beneficia as operações, a competitividade e o sucesso dos negócios. Isso é um retorno real sobre o investimento.
- **Verificar a postura atual.** Um processo de transição inteligente começa com uma avaliação de maturidade que descreve a atual postura de identidade da empresa. A maioria das organizações ainda está na fase inicial de sua jornada de identidade, com processos manuais e tecnologias fragmentadas. Acesse `www.sailpoint.com/identity-security-horizons` para avaliar sua maturidade de identidade.
- **Obter ganhos rápidos.** Qualquer especialista em gerenciamento de mudanças dirá que pequenas vitórias favorecem a adoção. Isso pode significar começar com áreas pequenas, talvez em um departamento e depois expandir a partir daí. Lembre-se de estabelecer também metas de longo prazo.
- **Escolher ferramentas e parceiros.** Antes, foram mencionadas tecnologias "fragmentadas". Você precisa do oposto: segurança de identidade unificada, uma plataforma que centraliza o acesso, oferece visibilidade de 360 graus e IA. Os parceiros também podem ajudá-lo a aproveitar ao máximo seu programa, com serviços de planejamento e consultoria, além de ajuda na implementação.
- **Criar uma checklist.** Para chegar até o ponto desejado, faça uma checklist para orientar seu planejamento e ajudar a escolher a solução certa. Descubra como a sua empresa pode estruturar um caso de negócios, como as soluções lidam com solicitações de acesso, como automatizam o provisionamento, como estão aproveitando a IA e o aprendizado de máquina, o que fazem em relação ao gerenciamento de senhas e como estão configuradas para a separação de tarefas. Para obter mais ideias de checklists, consulte o `Guia definitivo de checklist de segurança de identidade unificada da SailPoint`.
- **Medir o sucesso.** Como em qualquer melhoria de processo, não é possível medir o nível de sucesso alcançado sem ter critérios de medição. Tente contar quantas ações de controle de acesso você conseguiu automatizar. Ou a porcentagem de recursos simplificados e a economia de custos resultante. Ou, ainda, qual foi a redução no tempo de fornecimento de acesso.
- **Continuar aprendendo.** Este é um livro curto, onde foram incluídos todos os insights relevantes. Você poderá obter muito mais recursos e oportunidades de aprendizado visitando `www.sailpoint.com` e clicando na guia Recursos.

SailPoint

Segurança para todas as identidades. Controle para todos os acessos.

Boas-vindas ao centro da segurança empresarial

sailpoint.com/pt-br

Melhore a segurança de identidade, garantindo segurança e eficiência

À medida que as ameaças cibernéticas aumentam, a segurança de identidade moderna é fundamental para o sucesso das organizações. A segurança de identidade é eficaz em prevenir os ataques, melhorar a eficiência e diminuir os custos. Ela é o segredo para satisfazer tanto a equipe de risco/conformidade quanto os usuários, elevando a produtividade e garantindo a inovação que buscam os líderes de negócios. *Segurança de Identidade Moderna para Leigos* é o seu guia para criar uma segurança de identidade mais forte, gerenciar os ciclos de vida da identidade, conceder o acesso certo às pessoas certas e usar a IA para detectar ameaças e simplificar processos.

Abra este livro e descubra...

- O que significa segurança de identidade
- A diferença entre autenticação e autorização
- Os benefícios da segurança de identidade
- Como gerenciar todo o ciclo de vida da identidade
- Como estabelecer os controles certos de acesso
- Como automatizar processos com IA agêntica
- Como criar um roteiro de segurança de identidade

Steve Kaelble é autor de muitos livros da série *Para Leigos*. Seus textos também foram publicados em revistas, jornais, relatórios anuais corporativos e livros de mesa. Quando não está imerso no mundo de *Para Leigos* ou escrevendo artigos, ele se dedica a comunicações sobre saúde.

Acesse o site Dummies.com®
para obter vídeos, fotos passo a passo, artigos descritivos ou para compras!

ISBN: 978-1-394-37893-7

para leigos®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.