DOCUMENTAÇÃO TÉCNICA | MAIO DE 2017

Um modelo de maturidade do gerenciamento de acesso com privilégios para a transformação digital e a automação em escala

ca technologies

Sumário

Resumo executivo

Desafio

As organizações que estão passando por transformações digitais estão lidando com grandes preocupações em relação ao risco e à segurança, o que é natural. As iniciativas de transformação digital sempre resultam em mais pontos de acesso à infraestrutura da empresa, que estão fora dos controles existentes, acessíveis a um conjunto maior e mais diverso de identidades e espalhados por uma infraestrutura dinâmica e distribuída.

Oportunidade

Conhecer os usuários que têm privilégios significa conhecer seus riscos. As próprias ferramentas de gerenciamento de acesso com privilégios precisam dar suporte à automação no processo de autorização e viabilizar a escalabilidade por meio do suporte tanto a operações dinâmicas quanto a uma infraestrutura efêmera – como as contas administrativas da Amazon Web Services (AWS) para indivíduos.

Benefícios

Para identificar melhor os ataques que exploram o roubo de credenciais não basta acumular um volume maior de dados, é preciso incorporar dados mais relevantes sobre o comportamento dos usuários com privilégios, o que pode apontar mudanças significativas que representam riscos reais. Essa abordagem é reforçada por meio da integração com sistemas de governança de acesso com privilégios para permitir análise comportamental entre os usuários com funções semelhantes.

Seção 1

Introdução

O software está no cerne do modelo de funcionamento e concorrência das empresas de hoje. Não é de hoje que a tecnologia desempenha um papel fundamental na estratégia comercial. Porém, a transformação digital elevou as iniciativas de transformação e aceleração do ciclo de distribuição de software e dos processos de desenvolvimento de aplicativos para um patamar que atinge toda a empresa e cada vez mais se relaciona com outra grande preocupação executiva: a segurança cibernética.

A transformação envolve mudanças e, consequentemente, riscos. Conforme as empresas avançam em suas jornadas de transformação digital, os riscos se tornam mais pronunciados – a menos que elas tenham um plano para alinhar a governança e segurança de acesso às iniciativas e espelhar as prioridades de muitos planos de transformação digital:

- Viabilizar a automação com responsabilidade e visibilidade
- Promover a rapidez na entrega lado a lado com a proteção dos ativos corporativos
- Garantir escalabilidade com processos integrados de governança de acesso e detecção de ameaças

Para garantir a visibilidade e responsabilidade pela conformidade, segurança e governança e, ao mesmo tempo, permitir flexibilidade para a transformação digital, é necessária uma abordagem nova e mais alinhada a quem – e agora o que, sob a forma de aplicativos, serviços, máquinas e coisas – recebe o acesso com privilégios.

Da mesma forma que agora muitas empresas se empenham na definição de um mapa prático para as jornadas de transformação digital, as equipes de segurança precisam das ferramentas certas e de recursos de integração para automatizar, acelerar e ampliar o gerenciamento de acesso e a mitigação de riscos progressivamente de acordo com as necessidades dos negócios – sem novos investimentos significativos.

Seção 2

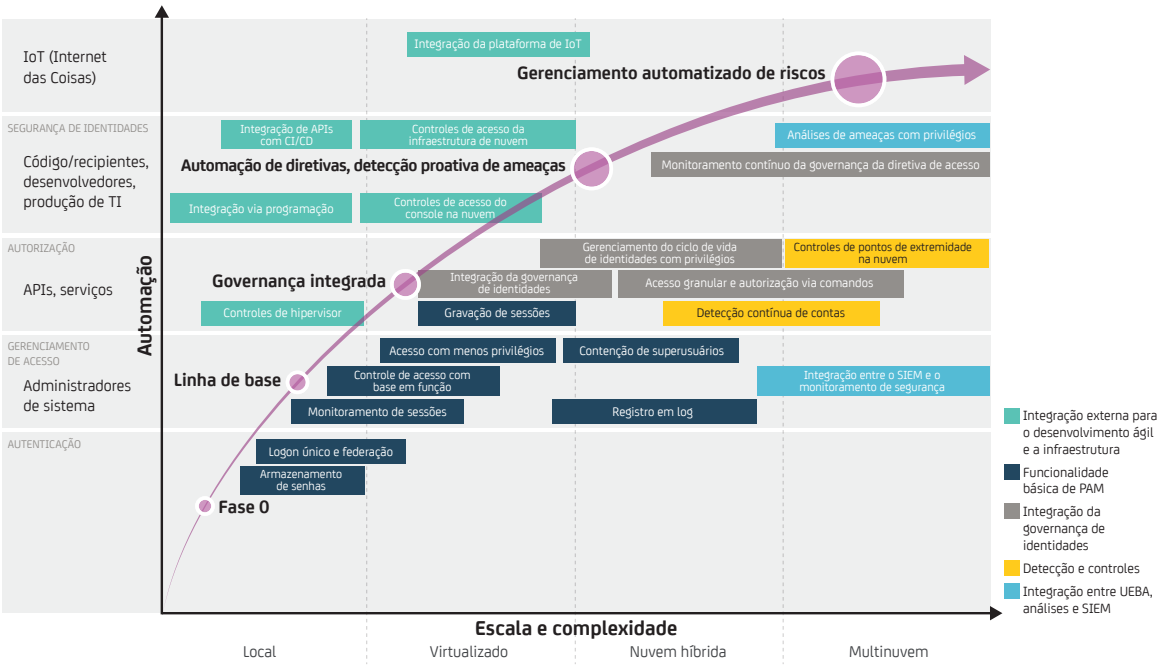
A transformação digital aumenta os riscos relacionados ao acesso com privilégios

A transformação digital obrigatoriamente muda, acelera e automatiza a forma como códigos, máquinas e indivíduos interagem entre si. Assim, as preocupações de risco e segurança se tornam maiores porque as iniciativas de transformação digital sempre resultam em mais pontos de acesso à infraestrutura da empresa, que estão fora dos controles existentes, acessíveis a um conjunto maior e mais diverso de identidades do que o anterior, e espalhados por uma infraestrutura dinâmica e distribuída (local, virtual e na nuvem).

O principal desafio quando se tenta viabilizar a automação, escalabilidade e rapidez é determinar quais identidades devem ter acesso a serviços e recursos específicos, gerenciar as credenciais delas para esses recursos e garantir que o acesso seja adequado com o mínimo de intervenção manual, tendo como base a diretiva.

Além disso, para lidar com a revolução da mobilidade, as empresas precisam se preparar para a IoT (Internet of Things – Internet das Coisas), que aumenta, em ordens de magnitude, o volume de transações na infraestrutura delas. Como resultado da adoção de ferramentas de transformação digital, o elemento "quem" da fórmula de gerenciamento de acesso passa por uma grande mudança – mesmo antes de os dispositivos de IoT entrarem em cena.

Para o gerenciamento de acesso com privilégios servir como um dos principais facilitadores da transformação digital, não um gargalo, a tecnologia e as ferramentas precisam oferecer uma solução consolidada e extensível para os riscos criados pela jornada de transformação.



Governança integrada

Não é possível ampliar as abordagens manuais que dependem de um processo humano de certificação quando a transformação digital aumenta o número de usuários que precisam de acesso com privilégios fora das funções tradicionais de administrador de sistema e o número de entidades que podem agir como identidades com privilégios. Para manter o equilíbrio entre agilidade e segurança para os novos cenários de acesso – sejam desenvolvedores com acesso a credenciais com privilégios na produção, em recipientes virtualizados e em hosts com autorização para fontes de dados ou administradores com acesso de superusuário aos serviços na nuvem –, as solicitações de autorização e função precisam ser gerenciadas por meio de um processo integrado de governança.

Automação de diretivas

As arquiteturas de implantação e desenvolvimento em nuvem híbrida que englobam recursos locais, datacenters virtualizados e ambientes de nuvem pública podem resultar em uma abordagem fragmentada e desconexa em relação às identidades com privilégios. A fim de garantir a consistência (e evitar o aprisionamento tecnológico), você deve aplicar diretivas centralizadas de controle de acesso e governança de maneira dinâmica às contas com privilégios específicas do ambiente (por exemplo, contas de superadministrador da AWS).

Detecção proativa de ameaças

Ao contrário do gerenciamento de acesso a uma senha compartilhada em uma infraestrutura estática, como um servidor de datacenter físico, agora as empresas precisam gerenciar a forma de autorizar, monitorar e registrar em log o acesso às credenciais com privilégios por um dia, uma hora ou mesmo minutos, além de avaliar se as alterações ou ações feitas com essas credenciais são legítimas e não elevam os riscos. A adoção de uma abordagem orientada ao contexto que utiliza aprendizado de máquina e análise comportamental pode proporcionar detecção em tempo real e acionar etapas de mitigação de riscos mesmo em ambientes dinâmicos e efêmeros.

Gerenciamento automatizado de riscos

A IoT não só introduz um novo tipo de identidade de máquina com privilégios sob a forma de controladores de dispositivo de IoT, mas seu uso também contribui para um aumento possivelmente exponencial no número de transações que devem ser autorizadas e monitoradas de maneira explícita quanto a possíveis ataques. Para lidar com a escala de identidades e o volume de transações por identidades com privilégios, é preciso um modelo automatizado que seja eficiente na detecção de ameaças e dê suporte a mecanismos para avaliar o risco e implementar a mitigação, sem interrupções significativas dos processos de negócios.

Seção 3

Obtenha governança integrada e automação de diretivas dando um passo de cada vez

O gerenciamento e a proteção do acesso com privilégios no contexto da transformação digital são um grande desafio, mas não insuperável.

Entretanto, com os invasores tirando cada vez mais proveito das credenciais de usuários com privilégios para obter acesso não autorizado (e tendo cada vez mais sucesso nisso), é preciso um modelo de maturidade para limitar a diretiva e monitorar os pontos cegos, bem como para permitir a criação de um modelo de detecção proativa por meio de uma análise orientada a aprendizado de máquina que possa reforçar o valor dos investimentos existentes e aumentar a precisão.

Para facilitar, em vez de impedir, a transformação digital, o acesso com privilégios à infraestrutura, bem como aos sistemas e dados confidenciais, deve ter como base um conjunto de fases realistas e coordenadas no contexto de um modelo de maturidade. A ação mais óbvia é reduzir o número de etapas manuais necessárias para fornecer acesso às credenciais com privilégios, além de vincular as decisões de autorização a diretivas claras.

Quanto mais integrados forem os processos de gerenciamento de acesso com privilégios e gerenciamento do ciclo de vida de identidades, maior será o escopo que as equipes de segurança terão para viabilizar a automação em escala. A aplicação de verificações automatizadas nas funções e autorizações de acesso atribuídas às identidades com privilégios pode ajudar a sinalizar violações de maneira proativa, por exemplo, um desenvolvedor que está recebendo acesso a credenciais para o código de produção.

O mais importante aqui é que as próprias ferramentas de gerenciamento de acesso com privilégios precisam dar suporte à automação no processo de autorização e viabilizar a escalabilidade por meio do suporte tanto a operações dinâmicas quanto a uma infraestrutura efêmera, como as contas administrativas da AWS para indivíduos.

Muitas das abordagens existentes em relação ao gerenciamento de acesso com privilégios se baseiam na cobertura de um subconjunto de identidades com privilégios e não foram projetadas com a infraestrutura moderna de TI em mente. Para avançar nas fases de um modelo de maturidade, as empresas precisam considerar como as abordagens de gerenciamento de acesso com privilégios lidam com o aumento, a distribuição e a transformação das identidades com privilégios em relação à capacidade de:

- Estender a governança e a visibilidade das identidades com privilégios da infraestrutura local aos datacenters virtualizados e aos serviços na nuvem.
- Automatizar a autorização de acesso com privilégios de acordo com os requisitos operacionais por meio da integração com diretivas de gerenciamento de identidades com base em função, não utilizando processos manuais de aprovação.
- Ampliar os controles e o monitoramento, bem como integrá-los à infraestrutura dinâmica e efêmera.
- Facilitar processos contínuos e centralizados de monitoramento e governança para identificar logo no início quando são concedidos privilégios em excesso e acionar um fluxo de trabalho de remediação.
- Incorporar, por meio de modelos orientados a dados e aprendizado de máquina, a capacidade de detectar e remediar novas ameaças conforme elas surgem.

Seção 4

Coloque os riscos no contexto certo

Como os programas de transformação digital resultam em redes distribuídas, altas taxas de alteração/volume transacional e aumento no número de identidades com privilégios, as abordagens tradicionais com base em regras têm dificuldade para detectar o uso indevido ou roubo de credenciais com privilégios – o que já foi provado inadequado mesmo para as ameaças existentes.

Se adotar uma abordagem geral em relação à análise de acesso com privilégios e empurrar mais dados para os sistemas de SIEM (Security Information and Event Management – Gerenciamento de Eventos e Informações de Segurança), você acabará perdendo um importante contexto que permite aos analistas de segurança e operadores de TI fazer uma distinção clara entre uma inconsistência, uma anomalia séria e uma atividade de alto risco que exige remediação.

Você precisa de uma abordagem específica de domínio que aproveite o contexto e o conhecimento sobre o comportamento e as funções dos usuários com privilégios para restringir o escopo e conseguir encontrar a agulha no palheiro, ou seja, as ações que representam provas tangíveis de um ataque ou comprometimento.

A abordagem específica de domínio funcionará com base nos mesmos princípios da definição de linhas de base de comportamento: quais ações os usuários com privilégios estão realizando, o que eles fizeram no passado e o nível ou risco associado a isso, incluindo a confidencialidade do recurso de destino, e como eles estão acessando os sistemas. No entanto, a abordagem também deverá incorporar uma relação de entidade de gráfico que coloque o comportamento dentro do contexto.

Seção 5

Conheça os usuários com privilégios, conheça seus riscos

Para identificar melhor os ataques que exploram o roubo de credenciais não basta acumular um volume maior de dados, é preciso incorporar dados mais relevantes sobre o comportamento dos usuários com privilégios, o que pode apontar mudanças significativas que representam riscos reais.

Essa abordagem é reforçada por meio da integração com sistemas de governança de acesso com privilégios para permitir análise comportamental entre os usuários com funções semelhantes. Assim, quando um usuário/uma máquina com privilégios acessa um sistema que não está de acordo com a função e os pontos correspondentes ou acessa um sistema compatível, mas a partir de um endereço IP diferente, e realiza ações que fogem do padrão anterior, o sistema consegue detectar de maneira mais precisa que o comportamento caracteriza um ataque e possibilitar a remediação adequada.

Seção 6

Conclusão

A transformação digital não é um processo que acontece da noite para o dia, mas sem dúvida dependerá da capacidade da empresa de automatizar tanto a aplicação da diretiva de segurança para as identidades com maior risco quanto a detecção de possíveis ameaças com base no uso indevido dessas identidades com privilégios. Implementar uma abordagem com base no risco significa garantir que a análise e os controles de segurança acompanharão o ritmo da jornada de transformação digital, bem como viabilizar a automação, escalabilidade e rapidez de maneira econômica sem qualquer comprometimento. Essa jornada exige um roteiro claro que se estenda por vários anos, antecipando requisitos de curto e longo prazo com base em uma solução de gerenciamento de acesso com privilégios, e garanta que as necessidades de escopo e escala serão atendidas a um custo total de propriedade razoável durante todo o ciclo de vida.

A segurança é fundamental, mas o escopo, a escala e os custos não podem se tornar um entrave para a transformação digital.

Para saber mais sobre como o CA PAM pode ajudar sua empresa, visite **ca.com/pam**

ca technologies

Conecte-se com a CA Technologies em ca.com/br

A CA Technologies (NASDAQ: CA) cria software que acelera a transformação das empresas e permite que elas aproveitem as oportunidades da economia dos aplicativos. O software está no cerne de todas as empresas, em todos os setores. Do planejamento ao desenvolvimento e do gerenciamento à segurança, a CA está trabalhando com empresas de todo o mundo para mudar a maneira como vivemos, fazemos negócios e nos comunicamos – usando dispositivos móveis, as nuvens privada e pública e os ambientes distribuídos e de mainframe. Obtenha mais informações em **ca.com/br**.

CS200-270334_0517