IBM Security

Um guia para otimizar a detecção de risco e a experiência em identidade digital com acesso adaptável

O poder da identidade

Nossas identidades digitais são fundamentais para a maneira como interagimos uns com os outros e com o mundo on-line.[1] A capacidade de provar quem somos nos dá controle e permite o acesso a pessoas, informações e economias. A confiança digital nessas identidades é poder.

Porém, criar uma identidade digital confiável pode ser difícil. É uma rede complexa de instrumentos tradicionais de identificação, como nome, endereço, data de aniversário e número do CPF, e pontos de dados, como endereço de e-mail, nome de usuário e senha, hábitos de pesquisa, comportamento de compra e assim por diante.

Essas informações de identificação pessoal (PII) são compostas pelos atributos exclusivos associados a um indivíduo e são a porta de entrada para todas as trocas on-line. Essas ações dependem do contexto para entender a identidade.

À medida que as trocas aumentam, no entanto, também aumentam as vulnerabilidades.[2] Os criminosos estão constantemente encontrando novas maneiras de explorar as PII's para roubar identidades ou de invadir empresas para roubar dados valiosos. Em 2018, o número de registros de consumidores expostos com PII's sensíveis subiu para 126%.[3] Em 2019, o prejuízo de um vazamento de dados aumentou para quase US$ 4 milhões.[4]

- *Números de telefone*
- *Endereços de e-mail*
- *Nome*
- *Uso do dispositivo*
- *Hábitos de pesquisa*
- *Comportamento de compra*
- *Dados geográficos*
- *Dados biométricos*
- *Velocidade do mouse*
- *Velocidade de digitação*
- *Endereço*
- *CPF*

Empurrando com a barriga

O problema é que as pessoas não entendem exatamente o que é a segurança virtual,[5] e muitas organizações ainda estão protegendo aplicativos críticos apenas com nome de usuário e senha, quando há uma forma melhor de fazer isso. A autenticação multifator (MFA) adiciona uma camada de segurança e dificulta muito o acesso de pessoas não autorizadas. Então, por que todo mundo está cobrindo os olhos e empurrando com a barriga?

Muitas vezes, as pessoas acreditam (por engano) que o risco de frustrar usuários finais, funcionários e clientes é maior do que um vazamento de dados. Apesar de um aumento esperado e de ser mais segura, apenas uma fração das organizações usa a MFA. De acordo com o Gartner, "até 2022, 60% das implementações de gerenciamento de acesso (AM) aproveitarão os recursos de análise de comportamento de usuários e entidades (UEBA) e outros controles para fornecer autenticação contínua, autorização e detecção de fraude on-line, acima dos 10% atuais".[6]

Apesar de um aumento esperado e de ser mais segura, apenas uma fração das organizações usa a MFA.

Experiência vs. segurança

Considere que os usuários comuns de negócios gerenciam (geralmente mal) 191 senhas,[7] com a mesma senha repetidamente. Como se essa quantidade já não fosse irritante o suficiente, experimente fazer com que eles esperem por um SMS ou e-mail com um código para fazer login.

Ou peça que identifiquem fotos com carros ou semáforos quando a maioria parecer ter as duas coisas. Em seguida, bombardeie os usuários com outro e-mail alertando sobre o acesso recente que eles fizeram, depois de passarem por tantas etapas, se é que conseguiram ir tão longe. Apenas 28% dos adultos dos EUA podem identificar um exemplo de autenticação de dois fatores.[8]

Estenda esse processo complicado aos clientes, e eles talvez nunca mais retornem. Hoje, a experiência é um diferencial importante, portanto, tratar os clientes como criminosos virtuais arrisca os resultados finais.

O gerenciamento de acesso não precisa ser uma situação de escolha. Quando é inteligente, a MFA funciona. A usabilidade e a segurança podem ser otimizadas se a segurança funcionar silenciosamente em segundo plano, reunindo contexto sobre o usuário e o comportamento. Ela então usa essa contexto para fornecer o processo de autenticação correto para a situação, criando experiências adaptáveis e descomplicadas.

Ponto-chave

Apenas 28% dos adultos dos EUA podem identificar um exemplo de autenticação de dois fatores.[8]

Pode olhar

Com um gerenciamento de acesso que aplica a MFA somente quando riscos são detectados, você melhora a experiência dos usuários. A confiança é criada com uma linha de contexto que começa com o usuário e flui para o dispositivo, a atividade, o ambiente de rede e o comportamento do usuário.

Pontuação de confiança

A detecção de riscos com IA usa modelos de aprendizado de máquina para sintetizar o contexto em dispositivos móveis, sessões da Web e VPNs com base em critérios como infratores, infecções por malware e outras anomalias para recomendar automaticamente a MFA em cenários de alto risco.

A análise de contexto combina fatores positivos e negativos para criar um único indicador de confiança. Essa pontuação leva sua estratégia de tudo ou nada para uma compreensão mais sutil do nível de confiança entre você e seus usuários. Essa flexibilidade serve de base para uma estratégia de acesso adaptável.

Quando você tenha uma pontuação de confiança, você não precisa mais confiar em regras estáticas para autenticação. Em vez disso, você pode criar uma estratégia de autenticação inteligente que ofereça acesso garantido aos usuários confiáveis e possa limitar o acesso à medida que o risco aumenta. Com essa abordagem, os usuários de baixo risco podem ter uma experiência sem senha e obter acesso sem nenhum esforço manual para avaliar as identidades deles.

Ponto-chave

A análise de contexto combina fatores positivos e negativos para criar um único indicador de confiança.

A autenticação inteligente determina:

- É uma pessoa ou um robô?
- Existe alguma evidência de ação mal-intencionada?
- O telefone é pré-pago, com root ou com jailbreak?
- O número do telefone ou e-mail são verdadeiros?
- Há um padrão de ações mal-intencionadas?
- A autenticação fora de banda foi ignorada?
- Existe um proxy de login?
- O padrão de comportamento do usuário é conhecido?
- Os movimentos do mouse parecem incomuns ou automatizados?

Pontuação de confiança: como funciona

Por exemplo, um usuário com algumas pequenas divergências pode ser autorizado com restrições em transações ou atividades. Usuários altamente confiáveis, com dispositivos conhecidos e pontuações biométricas comportamentais positivas, podem ter permissão para entrar sem senha.

Experimente a demonstração →

A promessa do acesso adaptável

As regras estáticas definem o nível de verificação como muito baixo ou muito alto. O IBM Security Verify com acesso adaptável é uma plataforma de gerenciamento de acesso inteligente que combina detecção avançada de riscos com um mecanismo de política de acesso robusto para avaliar o contexto completo da identidade de um usuário enquanto ele tenta acessar um serviço digital. A promessa de uma experiência digital sem frustrações pode ser cumprida sem sacrificar a segurança.

Para organizações que lutam para otimizar a detecção de risco de identidade e a facilidade de uso, o IBM Security Verify com acesso adaptável reduz as complexidades de autenticação, oferecendo acesso inteligente e gratuito a aplicativos e dados.

A solução é facilmente integrada a aplicativos com pouca ou nenhuma necessidade de programação, por meio de uma API para aplicativos personalizados e modelos pré-criados para os aplicativos mais usados na nuvem.

Ponto-chave

Para as organizações que lutam para otimizar o risco de identidade e a facilidade de uso, o IBM Security Verify com acesso adaptável reduz as complexidades de autenticação, oferecendo acesso inteligente e gratuito a aplicativos e dados.

A autenticação deve ser mais inteligente. A autenticação inteligente se adapta.

Próximas etapas

Saiba mais
Explore três formas diferentes de melhorar seu gerenciamento de identidade e acesso

Leia a postagem do blog

Experimente a demonstração interativa
Veja como o IBM Security Verify com acesso adaptável funciona no mundo real.

Experimente a demonstração

Ouça os especialistas
Saiba como estratégias de acesso adaptável podem melhorar a experiência do cliente e reduzir os riscos

Participe do webinar

Fontes

1. IBM, Gerenciamento de identidade digital: quanto de suas informações pessoais você controla?
2. IBM Institute for Business Value, Trust me: Identidade digital no blockchain, abril de 2017
3. Centro de Recursos para Roubo de Identidade, Consumidores em Risco: Aumento de 126% nos dados de consumidores expostos, 1,48 bilhão de credenciais relacionadas a e-mail, 28 de janeiro de 2019
4. IBM, O prejuízo de um vazamento de dados, 2019
5. Pew Research Center, O que o público sabe sobre segurança cibernética, Aaron Smith, 22 de março de 2017
6. Gartner, Quadrante Mágico de 2019 para Gerenciamento de Acesso. Abhyuday Data, Michael Kelly, Henrique Teixeira
7. Revista Security, usuário médio de negócios, possui 191 senhas, 6 de novembro de 2017
8. Pew Research Center, Americanos e o Conhecimento Digital, Monica Anderson e Emily Vogels, 9 de outubro de 2019

IBM