Whitepaper

Ficando sem senha

AWARE

781.687.0300 | sales@aware.com | www.aware.com

A Aware é líder mundial de produtos e soluções biométricas. As soluções de verificação e gerenciamento de identidade da Aware oferecem suporte a serviços financeiros, segurança corporativa, setor de saúde, recursos humanos, identificação civil, gerenciamento de fronteiras, segurança pública, defesa e inteligência. A tecnología da Aware ajuda organizações a coletar, gerenciar, processar e combinar imagens e dados biométricos em suas soluções de identificação e autenticação.

A pandemia do COVID-19 criou novos desafios para as empresas, pois foram forçadas a se adaptar a um modelo operacional em que trabalhar em casa era o novo normal. Essas condições de trabalho em casa resultaram em maior dependência da tecnologia e, sem a segurança da infraestrutura do escritório, muitos trabalhadores foram expostos a um número maior de riscos de ataques cibernéticos. Além disso, os funcionários estão enfrentando uma fadiga crescente de senhas resultante da necessidade de atualizar constantemente as senhas. Dado esse estado de fluxo, os métodos de autenticação atuais não são suficientes para proteger os dados da empresa e do trabalhador. A necessidade de uma autenticação mais forte é mais importante do que nunca.

Métodos de autenticação atuais

Com o aumento das ameaças à segurança cibernética, muitas empresas recorreram à autenticação de dois fatores. A autenticação de dois fatores é um método de autenticação eletrônica no qual um usuário recebe acesso a um site ou aplicativo somente após apresentar com sucesso duas evidências a um mecanismo de autenticação. Os fatores que concedem acesso incluem algo que você conhece – como senha, frase secreta ou número de identificação pessoal – e algo que você possui – como um dispositivo móvel ou uma chave USB segura.

Esse nível de autenticação tornou-se a norma porque permite que as organizações continuem a usar senhas. No entanto, o método está longe de ser perfeito. Muitos usuários relatam[1] que os obstáculos adicionais da autenticação de dois fatores são excessivamente inconvenientes, o que pode fazer com que usuários irritados cortem atalhos e tomem atalhos que tornam o sistema mais vulnerável. Embora exigir um identificador extra impeça alguns hackers de atacar sistemas defendidos com autenticação multifator, muitos outros estão dispostos a lidar com o obstáculo adicional se acreditarem que as informações armazenadas em sua organização alvo valem o esforço. Além disso, a autenticação de dois fatores não fornece autenticação de identidade, mas sim autenticação de dispositivo. O teste de posse do dispositivo é realizado sob a suposição de que o proprietário do dispositivo específico será o único indivíduo a usá-lo, não levando em consideração casos de fraude.

O problema da senha

À medida que o mundo continua a aumentar a dependência de soluções digitais, a sociedade continua a ser fortemente dependente de senhas e pins. Infelizmente, as senhas têm problemas. Na verdade, quase todos os profissionais de TI (~95%) concordam que as senhas representam riscos reais de segurança para sua organização. Isso ocorre porque as pessoas estão usando senhas fracas, manipulando incorretamente as senhas (escrevendo-as em post-its) e reutilizando aquelas com as quais os usuários se sentem confortáveis, entre outros maus hábitos. De acordo com Gartner[2], o Relatório de Comportamentos de Segurança de Senha e Autenticação 2020[3] e Verizon[4]:

- **20-50% de todas as chamadas de suporte técnico estão relacionadas a redefinições de senha**
- **39-50% das pessoas reutilizam senhas pessoais ou comerciais para contas no local de trabalho**
- **80% das violações envolveram senhas fracas ou roubadas**

Entre as maiores frustrações[5] para os funcionários está a troca de senhas, lembrar as 100 senhas anteriores e não poder reutilizá-las. Isso torna o gerenciamento de senhas uma parte tediosa do trabalho e certamente não adiciona nenhuma segurança se for feito de forma inadequada. Como resultado, muitos trabalhadores sofrem de fadiga de senha. A fadiga de senha pode ser definida como a luta para que os trabalhadores se lembrem de todas as suas senhas. Estima-se que o funcionário médio de uma empresa mantenha o controle de 191 senhas[6]. Este é um fardo óbvio. Os funcionários se cansam de ter que se lembrar de uma série de senhas, então começam a repeti-las e a reduzir a complexidade em um esforço para aliviar a carga mental de como fazer login. Infelizmente para muitos, o medo de esquecer uma senha supera o medo de uma possível violação de dados. De fato, 91% das pessoas[6] entendem o risco de reutilizar senhas, porém 59% admitem fazê-lo de qualquer maneira[6]. Em suma, as senhas são a porta de entrada para dados confidenciais, transações financeiras eletrônicas e muito mais, mas não as tratamos como o risco de segurança mais crítico que uma organização enfrenta. A fadiga de senhas, portanto, não afeta apenas os funcionários, mas também a segurança organizacional.

Queda claro que la empresa corre más riesgo si sus empleados están batallando con la fatiga de contraseña. De acuerdo con una encuesta conducida por el Ponemon Institute, 51% de las personas[7] alternan las mismas cinco contraseñas entre sus cuentas de trabajo y personales. Además de compartir las contraseñas entre sus propias cuentas, los empleados con frecuencia se comparten entre sí las contraseñas; 69% de las personas admiten que comparten credenciales para el acceso a la cuenta de trabajo. Otro riesgo de seguridad en potencia relacionado con la fatiga de contraseña es la susceptibilidad a la suplantación de identidad (phishing) ya que la mayoría de las solicitudes de recuperación de contraseñas se entregan por correo electrónico. La suplantación de identidad (phishing) es el vector de ataque más común y presente en 36%[4] de las filtraciones de datos. Si se suplanta con éxito la identidad de un empleado que sufre fatiga de contraseña, quien además tiene cinco contraseñas en rotación que comparte con otro compañero, la situación podría escalar con facilidad a una filtración de datos grave. Como resultado, muchas de las peores filtraciones de datos corporativos se han originado a través de transgresiones de contraseña.

Impacto do COVID-19 na tecnologia do local de trabalho

A pandemia de COVID-19 em curso destacou a fraqueza dos métodos de autenticação atuais, tornando a segurança cibernética uma prioridade crítica, pois milhões de trabalhadores e empresas em todo o mundo se tornam dependentes da infraestrutura digital e da Internet. De acordo com o Relatório de Riscos Globais de 2020[8], os líderes empresariais dizem que seus riscos de segurança cibernética estão aumentando com ataques cibernéticos e roubo de dados entre os 10 principais riscos que os CEOs provavelmente enfrentarão no curto e no longo prazo. Somente nos primeiros seis meses de 2019, as violações de dados expuseram 4,1 bilhões de registros[9], muitas vezes com milhões de credenciais em uma única violação lançada na web pública e escura. O custo médio de uma violação é estimado em $3,92 milhões[10], e em 2021 a perda financeira global associada ao cibercrime foi de $6 trilhões.

A dependência da tecnologia e da internet, combinada com o medo contínuo causado pela pandemia, criou o ambiente perfeito para os cibercriminosos prosperarem. Os trabalhadores mudaram os estilos e comportamentos de trabalho. Por exemplo, a HP Inc.[12] informou que 70% dos funcionários de escritório pesquisados admitem usar seus dispositivos de trabalho para tarefas pessoais, enquanto 69% usam laptops ou impressoras pessoais para atividades de trabalho. Como resultado desses fatores, os trabalhadores domésticos estavam cada vez mais sendo alvo de hackers. Os cibercriminosos conseguiram resgatar milhões de dólares de empresas usando táticas testadas pelo tempo, como phishing, engenharia social e outras ferramentas de hackers do comércio. Para as empresas, o custo médio de uma violação de dados subiu para US$ 21.659 por incidente durante a pandemia, com a maioria dos incidentes variando de US$ 800 a mais de US$ 650.000, segundo um novo relatório da Verizon[4]. Mas 5% dos ataques bem-sucedidos custam às empresas no mínimo US$ 1 milhão. A KuppingerCole[13] relata que houve um aumento de 238% no volume global de ataques cibernéticos durante a pandemia.

Reduza as taxas alarmantes de crimes cibernéticos com autenticação biométrica

As senhas foram inventadas na década de 1960 e nunca tiveram a intenção de proteger contas bancárias, registros de saúde, e-mails e uma longa lista de outros usos requisitados. Na verdade, eles foram inventados para o compartilhamento de tempo do computador e funcionaram com eficiência suficiente para esse caso de uso na época. O aumento das ameaças à segurança cibernética e a identificação falsa fizeram com que muitas empresas adotassem métodos rígidos, como autenticação de dois fatores, para combater esses problemas. No entanto, resolver problemas de identidade e segurança pode ser facilitado com a biometria. Isso ocorre porque a biometria pode ser simplificada nos métodos atuais de autenticação multifator ou permitir que os usuários abandonem completamente as senhas.

A autenticação multifator biométrica[14] funciona como os métodos atuais de autenticação de dois fatores, mas requer um fator adicional na sequência de login. Um dos fatores que o usuário final deve fornecer é uma biometria (por exemplo, face ou impressão digital). A tecnologia biométrica tornou-se o padrão ouro para segurança e prova de identidade devido às suas altas porcentagens de precisão. A adição de biometria na autenticação multifator pode tornar as senhas obsoletas, fortalecendo a infraestrutura de TI das empresas em todo o mundo. No mínimo, a biometria poderia fortalecer a autenticação multifatorial geral.

Até o final de 2022, Gartner[15] prevê que 60% das empresas grandes e globais e 90% das empresas de médio porte implementarão métodos sem senha em mais de 50% dos casos de uso – acima dos 5% em 2018. A autenticação sem senha[14], por sua natureza, elimina o problema de usar senhas fracas. Também oferece benefícios para usuários e organizações. Para os usuários, isso faz com que o crescente problema de fadiga de senha também se torne obsoleto.

Para as organizações, não há mais necessidade de armazenar senhas e, como resultado, as empresas terão:

Melhor segurança:

embora as senhas sejam vulneráveis a tentativas de phishing, a biometria e os tokens de hardware não são. A autenticação sem senha remove o problema de senhas duplicadas e práticas de gerenciamento de senha abaixo da média, como escrever códigos em notas adesivas

Menos violações:

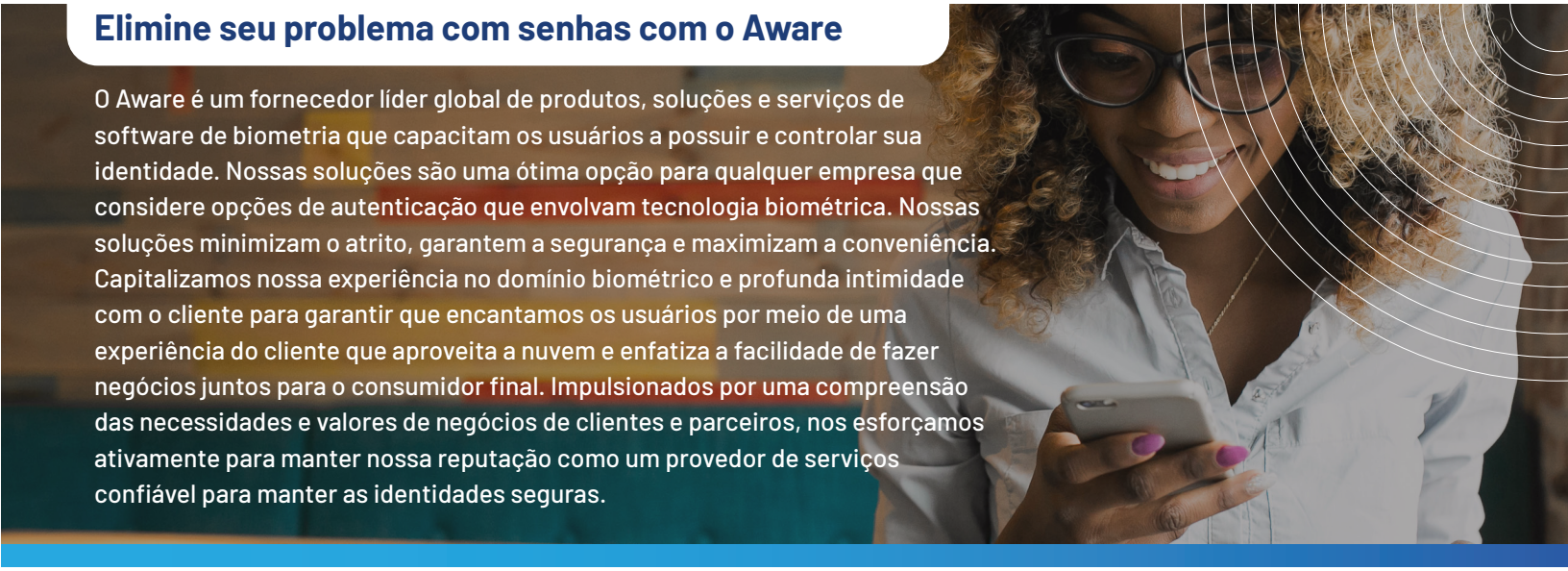
quando as empresas migram para soluções sem senha, elas reduzem consideravelmente sua exposição a violações de dados. Ao usar soluções sem senha para autenticação, não há senhas para os cibercriminosos roubarem de um servidor de plataforma.

Custos de suporte mais baixos:

a autenticação sem senha é mais barata a longo prazo. As senhas exigem que as organizações mantenham sistemas de gerenciamento de senhas para que os usuários possam realizar atualizações periódicas de senhas e redefinições de senhas ocasionais. Mudar a autenticação para a biometria, alivia a carga nos helpdesks e permite que as organizações economizem nos custos associados à substituição de senhas.

Com a crescente dependência da tecnologia, novas condições de trabalho e uma escalada cada vez maior de ataques cibernéticos maliciosos, este é o momento ideal para as empresas considerarem a atualização de seus produtos e procedimentos de segurança. A biometria agrega conveniência e segurança, permitindo que as empresas protejam seus dados. - seu ativo mais importante.

Elimine seu problema com senhas com o Aware



O Aware é um fornecedor líder global de produtos, soluções e serviços de software de biometria que capacitam os usuários a possuir e controlar sua identidade. Nossas soluções são uma ótima opção para qualquer empresa que considere opções de autenticação que envolvam tecnologia biométrica. Nossas soluções minimizam o atrito, garantem a segurança e maximizam a conveniência. Capitalizamos nossa experiência no domínio biométrico e profunda intimidade com o cliente para garantir que encantamos os usuários por meio de uma experiência do cliente que aproveita a nuvem e enfatiza a facilidade de fazer negócios juntos para o consumidor final. Impulsionados por uma compreensão das necessidades e valores de negócios de clientes e parceiros, nos esforçamos ativamente para manter nossa reputação como um provedor de serviços confiável para manter as identidades seguras.

Integração móvel: Nossas soluções fornecem prova de identidade para dar suporte à integração móvel. As verificações de segurança avançadas podem autenticar carteiras de motorista e passaportes e garantir correspondência facial biométrica resistente a falsificação entre imagens ao vivo e impressas. A integração inclui correspondência facial biométrica com documentos de identificação e verificação de mais de 9.000 documentos em todo o mundo. A detecção de vivacidade também detecta impostores, impedindo-os de acessar contas e informações confidenciais

Autenticação móvel: Nossa solução fornece autenticação multifator sem senha usando reconhecimento biométrico facial e de voz e detecção de vivacidade e é baseada em algoritmos de correspondência de rosto e voz testados pelo NIST. Com nossos recursos biométricos multimodais, os usuários podem ser autenticados com seus rostos, vozes ou uma combinação dos dois para uma segurança ainda maior.

Detecção de vivacidade: Nossos algoritmos avançados de detecção de ataques de apresentação detectam não apenas a representação da vítima, mas também a ocultação de identidade, proporcionando aos bancos e empresas financeiras a tranquilidade de saber que seus clientes são quem dizem ser. Nossa detecção de vivacidade também é passiva para os usuários, não exigindo etapas adicionais (como movimentos de cabeça solicitados) para ser eficaz. Nossa vivacidade funciona para integração e autenticação.

Configurações Flexíveis: Além de oferecer suporte a uma gama completa de sistemas operacionais móveis e baseados em servidor, nossas soluções podem ser configuradas para estarem disponíveis em dispositivos centrados, centrados em servidor ou baseados em navegador. As configurações baseadas em dispositivo colocam a funcionalidade biométrica no dispositivo de uma pessoa e são ideais para situações em que a disponibilidade da rede não é garantida. As configurações baseadas em servidor, no entanto, colocam a funcionalidade biométrica no servidor; uma solução perfeita para quando a disponibilidade da rede é forte. Nossas configurações baseadas em navegador funcionam como uma terceira opção, realizando a captura biométrica diretamente por meio de um navegador e colocando funcionalidades adicionais no servidor. Seja qual for a escolha, nossas soluções continuarão a oferecer o mesmo nível de segurança e conveniência.

Para mais informações sobre nosso portfólio biométrico, entre em contato conosco abaixo.

AWARE

Fontes:

1 https://medium.com/@rezaduty/2fa-security-issue-675a6dec825a
2 https://www.gartner.com/en/documents/3773163
3 https://www.yubico.com/blog/yubico-releases-2020-state-of-password-and-authentication-security-behaviors-report/
4 https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf
5 https://www.comparitech.com/blog/information-security/password-statistics/
6 https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-Enterprise-The-Password-Expose-Ebook-v2.pdf
7 https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Report-Infographic.pdf
8 https://www.weforum.org/reports/the-global-risks-report-2020
9 https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=4e662ce4bd54
10 https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years
11 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
12 https://threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/
13 https://www.kuppingercole.com/research/lc80127/fraud-reduction-intelligence-platforms
14 https://www.aware.com/blog-enhance-multifactor-authentication-enterprise/
15 https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security
16 https://www.aware.com/blog-going-passwordless/