REDEFININDO A Segurança das Senhas

Escrito por Julia O'Toole
Fundadora & CEO da MyCena Limited

À medida que nosso mundo se torna cada vez mais digital, precisamos de mais e mais senhas. Até há bem pouco tempo, podíamos contar com apenas algumas senhas. Hoje, a maioria dos usuários da Internet tem mais de 100 senhas.

Um mundo cada vez mais digital significa que o uso de senhas excederá os 300 bilhões até 2020[1].

À medida que nosso mundo se torna cada vez mais digital, precisamos de mais e mais senhas. Até há bem pouco tempo, podíamos contar com apenas algumas senhas. Hoje, a maioria dos usuários da Internet tem mais de 100 senhas.

E o problema está crescendo. Um relatório recente afirma que o uso de senhas está aumentando rapidamente e é provável que exceda os 300 bilhões até 2020[1].

Este documento explora o cenário da segurança das senhas, desde a compreensão dos usuários sobre a utilização de senhas à introdução de uma nova forma de proteger suas senhas para se proteger.

1. Cybersecurity Ventures The World Will Need to Protect 300 Billion Passwords by 2020 https://www.inc.com/joseph-steinberg/300-billion-thats-how-many-passwords-may-be-in-use-by-2020.html

Em primeiro lugar por que existem as senhas

As senhas são as chaves que abrem as portas ao nosso mundo digital. Assim como as nossas chaves abrem as portas do nosso espaço físico, as senhas abrem as portas do nosso espaço digital. Foram criadas para oferecer uma forma simples de provar nossa identidade ao usar sites, contas de email e aplicativos. As senhas são de fato a nossa primeira linha de defesa contra intrusos.

As senhas são as chaves que abrem a porta da frente para o nosso mundo digital

Por que as senhas já não protegem suas portas

Contudo, as senhas já não cumprem a sua função. De fato, um Relatório de Investigação de Violação de Dados da Verizon mostra que 81% das violações de dados são resultado de falhas de senhas, devido a senhas fracas, reutilizadas ou até roubadas [1].

Por que continuamos a usar senhas de alto risco

A nossa crescente dependência de aplicativos móveis e da Internet levou a um aumento no número de senhas. De simples contas de email a serviços bancários online, somos confrontados com centenas de senhas para usar.

Embora saibamos que precisamos usar senhas fortes, simplesmente não conseguimos lembrar de centenas de caracteres como £45@fag54hF8sD* para desbloquear cada porta. Como resultado, tendemos a usar combinações únicas, como 'nome1234' ou uma única senha com variações.

10% das pessoas usaram pelo menos uma das 25 piores senhas

As dez piores senhas de 2018

A lista anual das piores senhas do ano da SplashData[2] revela que os usuários de computador continuam utilizando as mesmas senhas previsíveis e fáceis de adivinhar, apesar do risco significativo de serem invadidos e de que lhes roubem suas identidades. Quase 10% das pessoas usaram pelo menos uma das 25 piores senhas da lista deste ano - e quase 3% usaram a pior senha, 123456.

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. Sunshine
9. Qwerty
10. iloveyou


Uma senha fraca é como não ter nenhuma senha

Além disso, a maioria de nós usa regularmente os seguintes métodos perigosos para armazenar as senhas [3] :

- 53% Confia na memória humana
- 32% Guarda-as num navegador web
- 26% Utiliza-se de planilhas
- 26% Anota-as
- 1% Outro

1. Verizon Data Breach Investigations Report https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/
2. SplashData's Top 100 Worst Passwords of 2018 https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/
3. Cyber Security Breaches Survey 2018 from the Department for Digital, Culture, Media and Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Por que as senhas são uma grande ameaça para as empresas

Como atuam os hackers

Você tem que saber como um hacker pensa para evitar ser invadido

Para entender por que as senhas são uma ameaça à segurança é importante entender como atuam os hackers.

- Phishing – os hackers podem se passar por contatos genuínos, por exemplo, bancos, para convencer os usuários a entregar suas credenciais.
- Engenharia social – os hackers extraem informações do seu perfil e atividades online para roubo de identidade.
- Credential stuffing – os hackers normalmente usam nomes de usuário e senhas roubados de uma violação de dados para tentar abrir outras contas usando ferramentas de automação da web.
- Força bruta – os hackers executam scripts para testar combinações de credenciais para "adivinhar" sua senha.

Uma alternativa denominada spidering é quando os hackers estudam uma empresa e aprendem a sua linguagem. Estes ataques são geralmente direcionados a grandes empresas com muitas informações disponíveis online. É frequentemente usado para obter acesso a senhas de Wi-Fi, pois muitos roteadores de escritório são protegidos por uma senha relacionada à empresa, como "Empresa1234".

Mais de 90% dos ataques são realizados por bots, que "enchem" ou "pulverizam" novas combinações. Esses robôs usam as informações de identidade divulgadas e as informações de perfil de mídias sociais para "adivinhar" mais rapidamente. A maioria das senhas pode ser decifrada em menos de 24 horas usando uma ferramenta de força bruta que pode ser baixada gratuitamente.

As Coleções #2–5 representam 845 gigabytes ou 2,2 bilhões de identidades roubadas, incluindo nomes de usuário e senhas.

Por que a transformação digital aumenta as vulnerabilidades

Enquanto mais de 60% das empresas da Fortune 500 passaram por uma transformação digital, permitindo uma força de trabalho mais colaborativa, suas redes conectadas também se tornaram o “sonho dos hackers”. A sua superfície de ataque é agora toda a equipe. De diretores-executivos a simples funcionários, qualquer pessoa que esteja conectada ao sistema está vulnerável a ataques cibernéticos e apresenta um risco potencial.

Paralelamente, como os usuários profissionais precisam de mais e mais contas, é mais provável que reutilizem senhas de várias contas, o que aumenta o risco de invasão. Por outro lado, as empresas que utilizam a conveniência do sistema Single Sign On (SSO) são vulneráveis a ataques de hackers que violam suas redes de informações e bancos de dados a partir de um ponto de acesso.

Portanto, não é uma surpresa que o número de roubos de identidade aumente. O ano de 2018 foi o pior ano já registrado em matéria de violações da segurança cibernética, seguido pelos dois dos maiores vazamentos de nomes de usuário e senhas da história, chamados Collection#1[1] e Collections #2-5[2] em janeiro de 2019. Atualmente, existem mais de 3 bilhões de identificadores de login e senhas à venda online e esse número continua aumentando diariamente.

Suas senhas são vulneráveis ao preenchimento de credenciais, phishing, engenharia social

1. Forbes https://www.forbes.com/sites/kateoflahertyuk/2019/01/17/collection-1-breach-how-to-find-out-if-your-password-has-been-stolen/#3c2d829a2a2e
2. Wired https://www.wired.com/story/collection-leak-usernames-passwords-billions/

Por que as novas leis de proteção de dados afetam todos os negócios

De pequenas empresas a grandes corporações, todas as empresas de todos os setores precisam de senhas fortes para proteger seus dados e os de seus clientes.

Com as leis de privacidade e proteção de dados como a RGPD em vigor em todo o mundo, as consequências financeiras de não proteger os dados e a privacidade dos clientes podem ser devastadoras, já que as empresas estão sujeitas a multas de até €20.000.000 ou 4% de seu facturamento global total.

Os ataques de spidering consistem em estudar uma empresa e escolher a sua linguagem, por exemplo empresa1234

O risco de ser um "peixe graúdo"

A indústria de hackers é composta por uma ampla gama de perfis, de criminosos não sofisticados a experts. Enquanto alguns hackers se estendem a outras redes, outros se concentram em metas de renda mais alta em setores mais estratégicos.

Violações em setores como defesa civil, polícia, governo, energia, água, serviços públicos, infraestrutura, tecnologia, telecomunicações, universidades, bancos, serviços financeiros, saúde, produtos farmacêuticos, transporte, logística, varejo ou leis podem ter efeitos devastadores.

Em maio de 2017, o ataque de ransomware WannaCry levou ao cancelamento de 19.000 operações médicas e consultas no Reino Unido, custando ao Serviço Nacional de Saúde (NHS) £92 milhões em interrupção a serviços e TI[1]. E em setembro de 2019, quase toda a população do Equador viu os seus dados pessoais divulgados[2].

A agora extinta Nortel foi alvo de um ataque de vários anos por hackers chineses patrocinados pelo Estado

Quando um “peixe graúdo” é violado, inevitavelmente também afeta fornecedores, parceiros e clientes. Em março de 2019, uma violação de dados da Citrix teve o potencial de afetar o acesso à rede privada virtual e credenciais de 400.000 empresas em todo o mundo, incluindo 98% das empresas da Fortune 500[3].

Na era da guerra cibernética, existem provas esmagadoras que alguns ataques são patrocinados pelo Estado. Países como a Coreia do Norte, Irão e China são famosos pelos seus ataques cibernéticos e furtos de propriedade intelectual.

Por exemplo, a agora extinta empresa canadense de telecomunicações Nortel foi alvo de um ataque de vários anos no qual os hackers roubaram senhas de executivos importantes para acessar a e-mails, pesquisas , planos de negócios e segredos comerciais. Os ataques foram então atribuídos a hackers patrocinados pelo Estado na China[4].

As empresas nem sempre percebem que há uma violação

Muitas empresas não identificam uma violação de segurança cibernética quando ocorre, sendo que 93% das violações de dados não sendo descobertas durante semanas[5].

As violações de dados podem não ser descobertas durante semanas

Nesse meio tempo, uma enorme quantidade de danos pode ser feita. Os hackers podem instalar malware no computador de um funcionário que pode extrair informações confidenciais da rede da empresa antes que a empresa perceba que sua segurança foi violada.

1. Department of Health and Social Care https://www.hsj.co.uk/technology-and-innovation/cyber-attack-cost-nhs-92m-dhsc/7023560.article
2. The New York Times https://www.nytimes.com/2019/09/17/world/americas/ecuador-data-leak.html
3. Forbes https://www.forbes.com/sites/kateoflahertyuk/2019/03/10/citrix-data-breach-heres-what-to-do-next/#47a1e6b11476
4. The Register https://www.theregister.co.uk/2012/02/15/nortel_breach/
5. Verdict https://www.verdict.co.uk/password-security-surveillance-fears/

Sua empresa leva a segurança cibernética a sério?

As empresas podem ter boas intenções, mas isso nem sempre se reflete em suas práticas. 74% das empresas e 53% das instituições de caridade relatam que a cibersegurança é a principal prioridade para a gestão de suas organizações. Apesar disso, ainda vemos:

- Apenas 27% das empresas e 21% das instituições de caridade têm uma política formal de segurança cibernética[1].
- Apenas 9% das empresas têm uma apólice de seguro de segurança cibernética em vigor.

Equilibrando a prevenção, monitoramento e recuperação

Com mais e mais ataques todos os dias, não se trata de saber se, mas quando seus negócios serão direcionados. Os CISOs estão sob crescente pressão para limitar o risco com recursos limitados. (Confuso, não entendi) Atualmente, cerca de 99% dos gastos corporativos com segurança cibernética são gastos em monitoramento e vigilância. No entanto, mesmo os melhores sistemas de monitoramento e vigilância não protegem sua empresa contra roubos de senhas.

Embora 80% dos riscos estejam relacionados com senhas, o gerenciamento de senhas representou apenas 0,53% dos gastos totais com segurança cibernética em 2017, um número que deve aumentar para apenas 0,58% por volta de 2023[2]. Para ajudar a proteger seus funcionários, clientes e comunidades em geral contra ameaças à segurança, as empresas devem priorizar a prevenção e organizar melhor a sua primeira linha de defesa.

Como impedir que sofra uma violação de dados através de senhas

Um primeiro passo seria configurar um sistema IAM (Gerenciamento de Identidades e Acessos) que permita aos gerentes atribuir diferentes níveis de acesso a diferentes usuários dentro de uma organização. Esta pode não ser a primeira preocupação para empresas menores, especialmente as que não têm um CISO.

Um segundo passo seria configurar um sistema de gerenciamento de senhas conveniente e seguro para impedir que os usuários usem senhas fracas ou reutilizadas. Muitas empresas falham nessa área porque possuem um sistema de senhas com falhas, o que aumenta o risco de ataques.

Em seu relatório, a SplashData dá às empresas o seguinte conselho para se protegerem contra hackers online:

- Use frases de 12 caracteres ou mais com diferentes tipos de caracteres.
- Use uma senha diferente para cada uma das suas conexões para que se um hacker acessar uma de suas senhas, não poderá usá-la para acessar outros sites.
- Proteja seus ativos e identidade pessoal usando um gerenciador de senhas para organizar senhas, gerar senhas seguras e aleatórias e entrar automaticamente em sites.

1. Cyber Security Breaches Survey 2018 from the Department for Digital, Culture, Media and Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
2. Stratistics MRC https://www.strategymrc.com/report/password-management-market-2017 https://www.strategymrc.com/report/cyber-security-market https://www.strategymrc.com/report/cyber-security-market-2016; MyCena estimates

Compreensão dos riscos associados aos gerenciadores de senhas centralizados na nuvem

Ao oferecer um método centralizado de armazenamento de senhas, os gerenciadores de senhas baseados na nuvem tornaram-se cada vez mais populares nos últimos anos. O que ocorre principalmente porque:

- Ajudam a gerar senhas fortes - só precisa se lembrar de uma senha principal. Digita sua senha mestra e acessa todas as outras senhas armazenadas na nuvem.
- Oferecem uma alternativa muito mais segura ao uso de post-its ou senhas fracas, como 123456.

Um gerenciador de senhas baseado em nuvem é conveniente, mas arriscado

Embora os gerenciadores de senhas baseados na nuvem possam ser práticos, sua arquitetura possui três riscos principais:

- Primeiro, por construção, todas as suas senhas são centralizadas e acessadas através de uma senha mestra, que se torna um ponto único de vulnerabilidade. Imagine que se essa senha mestre for comprometida de alguma forma, expõe todas as suas senhas de uma só vez. Pode pensar em uma senha mestra como a chave de um gerente de hotel. Um hacker precisa apenas dessa chave para acessar a todos os quartos. Para muitas empresas, não é um risco que possam correr.
- Segundo, todas as suas senhas estão na nuvem, centralizadas, da mesma forma que milhões de senhas de outros usuários. Este é um enorme imã para hackers, que são atraídos como abelhas para um pote de mel e farão todas as tentativas para invadir e roubar o banco.
- Terceiro, os servidores podem e são violados, seja por senhas ou outras vulnerabilidades. Gostaria de sair de casa com alguém que não conhece? Então por que o faz com suas chaves digitais? Ao deixá-las na nuvem é exatamente o que acontece.

Sua senha mestra é como a chave do castelo

Redefinindo as regras de segurança da senha

Um problema bem definido é um problema parcialmente resolvido. Para encontrar uma solução, devemos resolver o problema a partir do zero e repensar as regras que permitiam que as senhas cumprissem seu papel de primeira camada de segurança. Encontramos três regras principais:

Redefinindo as regras de segurança da senha

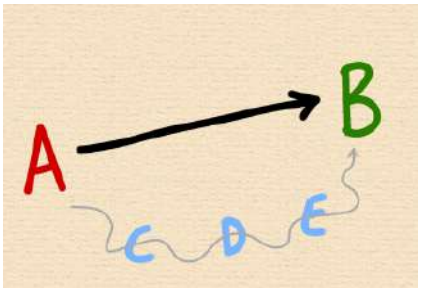
- As senhas são como chaves. Assim como você não precisa se lembrar como moldar as suas chaves sempre que quer abrir uma porta, também não precisa se lembrar de suas senhas para abrir suas portas digitais.
- As senhas devem ser privadas e acessíveis apenas ao proprietário e a mais ninguém.
- As senhas não devem ser vulneráveis em nenhum ponto de acesso

As lições da neurociência: compreender a conveniência

Para conseguir a adoção e o uso de qualquer nova tecnologia, a conveniência é fundamental. Esta regra aplica-se à segurança. Se demorar muito para abrir uma porta várias vezes ao dia, a maioria das pessoas deixará de trancá-la adequadamente. Portanto, a segurança só pode ser garantida se os sistemas e procedimentos que a entregam puderem ser aplicados sem problemas.

Nos últimos vinte anos, a neurociência nos ensinou muito sobre como nosso cérebro funciona. Uma descoberta importante é que nosso cérebro tende a seguir a forma mais simples de viajar de A a B. Aqui estão alguns exemplos:

- Quando se trata de encontrar um objeto, é muito mais eficiente para o cérebro lembrar-se de um local típico em que normalmente coloca esse objeto, em vez de se lembrar exatamente de onde o objeto está.
- É mais fácil para o cérebro seguir padrões conhecidos ou reconhecíveis do que criar novos. Isso explica por que o cérebro não é tão bom em criar novas senhas aleatórias.
- Nosso cérebro é visual e tende a combinar o que procura com objetos e modelos vistos antes.



O cérebro tende a voltar ao caminho mais fácil

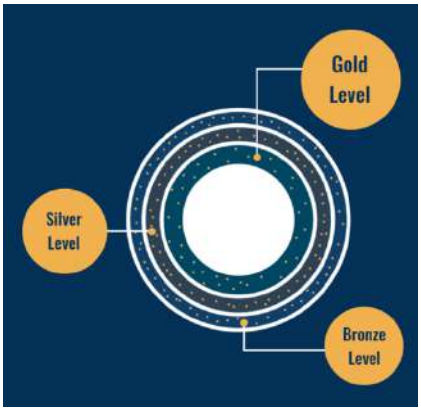
Faça as senhas funcionarem novamente

Depois de definir o problema, ainda temos que resolvê-lo.

Método de acesso a dados armazenados estruturados (dados MASS), com patente internacional pendente

Os dados MASS são uma solução inovadora que permite que as senhas sejam localizadas e descentralizadas, distribuindo e reduzindo o risco de perder tudo de uma vez. Esta solução permite a criação de vários níveis de segurança para armazenar senhas, dependendo da sua sensibilidade, com autenticação local em vários níveis e controle total do usuário sobre as senhas e configurações de segurança.

- Sem armazenamento na nuvem.
- Sem senha mestra.
- Sem qualquer ponto de vulnerabilidade.



Dados MASS: Cofre local de senhas multicamadas dentro do seu dispositivo

Prenda a conveniência para assegurar a segurança

A cibersegurança é responsabilidade de todos. Para ser amplamente adotada, a solução deve ser rápida, conveniente e fácil de usar.

- Permite ao proprietário da senha comprovar sua identidade de forma fácil e segura em cada nível para acessar suas senhas a qualquer momento, em qualquer lugar, com uma combinação de impressão digital, identidade facial, PIN, padrão de bloqueio e senha de voz.
- Gera senhas fortes por padrão.
- Permite localizar, copiar e colar senhas sem precisar digitar, redigitar ou ver qualquer senha.

A conveniência é fundamental - crie, salve, encontre, copie e cole senhas em segundos

Construir uma solução de nível corporativo

Para se adaptar ao ambiente empresarial, a solução necessita ser facilmente implantada e usada. Consiste em duas partes:

- Um console através do qual o gerente pode integrar rapidamente todos os funcionários, fortalecer e monitorar as políticas de senha, como a configuração do tamanho da senha, a frequência de alteração da senha e alertas para senhas fracas.
- Um aplicativo móvel usado pelos funcionários para acessar suas senhas com rapidez e segurança, inclui funcionalidades como vários dispositivos, várias plataformas, integração de desktop, modo de viagem, sincronização, migração, lembretes de backup automatizados e compartilhamento seguro de senhas.

Um console que permite que os gerentes reforcem as políticas de senha e monitorem a sua conformidade

Respeita a privacidade por defeito

Após muitos anos de erosão da privacidade, os legisladores fortaleceram as leis de privacidade para proteger as nossas sociedades e liberdades individuais. Apoiamos profundamente essa tendência. De fato, a nossa solução está construída com base num padrão de privacidade.

As senhas são criptografadas no seu dispositivo usando a criptografia AES-SHA 256. Isso significa que, mesmo que perca o dispositivo, o ladrão continuará a não poder acessar suas senhas. A única pessoa que pode reenviar o backup de suas senhas criptografadas é você.

Seus dados biométricos, como impressões digitais e identificação facial, são ainda mais sensíveis. Você pode alterar uma senha, mas não pode alterar seu rosto ou dedo. Portanto, qualquer autenticação pessoal é armazenada dentro do seu dispositivo local, sem nenhum repositório central de dados biométricos na nuvem, disponível a qualquer pessoa.

Privacidade por padrão: nunca mais veja ou digite uma senha

Limita os danos causados pelo phishing

É possível que nunca mais necessite ver uma senha novamente. Isso significa que, desde a criação das suas senhas até à sua utilização, através da opção "copiar e colar", nunca é necessário que haja um momento em que tenha que mostrar ou digitar suas senhas , o que limita as possibilidades de introduzir uma senha errada ou que alguém atrás de você espie a sua senha e a roube.

Mesmo que um hacker consiga convencê-lo a colar uma senha em seu site falso, roubando-a, essa senha não poderá ser reutilizada para entrar em outras contas, pois todas as suas senhas são únicas e fortes. Portanto, a sua rede completa não está exposta a nenhum ato de invasão.

Age como sua primeira linha de defesa

Uma vez que a solução é implementada dentro de uma organização, ela se torna de fato sua primeira linha de defesa. Para inserir qualquer aplicativo ou rede protegida por senha em uma empresa, o funcionário deve primeiro provar sua identidade em seu próprio dispositivo. Somente então podem acessar a senha forte e exclusiva que procuram. Essa senha forte e exclusiva provará que o funcionário tem o direito (porque possui a chave exclusiva) a acessar a esse aplicativo ou rede.

Atua como sua primeira linha de defesa

Descubra a solução de segurança de senhas descentralizada MyCena

Descubra o MyCena

O MyCena Business Fortress é uma solução revolucionária de segurança de senha de nível empresarial, descentralizada, fácil de implementar, conveniente e segura. Aprenda a instalar e configurar o MyCena facilmente para a sua empresa.

O MyCena Personal Fortress é um aplicativo revolucionário de segurança de senhas pessoais que os usuários individuais podem baixar em seu dispositivo móvel. Aprenda a proteger suas senhas com o MyCena Personal Fortress.

O MyCena como um Serviço

O MyCena como Serviço (MaaS) é um pacote de serviços completo que oferece o melhor da solução com suporte avançado, reduzindo o esforço para implementar e gerenciar a solução na empresa e seus funcionários.

Conclusões

A cibersegurança é a maior ameaça para as organizações. O número de violações de dados aumenta diariamente, resultando em multas, ações judiciais e ações corretivas, além de prejudicar irreversivelmente a reputação da empresa e a confiança dos clientes.

Para proteger suas empresas, os quadros superiores e executivos necessitam entender de onde vêm as ameaças e tomar ações decisivas. Como 81% das violações começam com senhas, a proteção por senha já não é apenas mais uma opção, é uma obrigatoriedade.

Os CISOs das empresas podem reduzir os riscos direcionando e ajudando seus funcionários a usar senhas fortes e exclusivas como sua primeira linha de defesa e descentralizar o armazenamento de senhas com o MyCena Business Fortress. Os CIOs também podem atenuar os riscos de violações de dados aproveitando o MyCena como um Serviço.

Para mais informações, entre em contato
support@MyCena.co

Visite o nosso site para mais informações
Versão teste grátis disponível
https://MyCena.co

Faça o download na Appstore ou no Google Play.