Departamento Estudos e Investigação em Tecnologias de Informação e Sociedade

kriativ.tech

Edição Nº 6 – 28 de Abril de 2018
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
DOI: https://doi.org/10.31112/kriativ-tech-2018-01-18
http://www.kriativ-tech.com http://www.kriativ-tech.pt

Cybersecurity: a importância das passwords

Pedro Ramos Brandão
Professor Coordenador do ISTEC
ISTEC – Departamento de Estudos e Investigação em Tecnologias de Informação e Sociedade
Investigador da Universidade de Évora – CIDEHUS
pedro.brandao@istec.pt *ORCID: https://orcid.org/0000-0001-6351-6272*

Resumo: O problema da simplificação das passwords. Os perigos da repetição da mesma password em vários sistemas. Análise dos principais métodos utilizados pelos hackers para conseguirem acesso a informação pessoal. Soluções para segurança das passwords. Passwords seguras.

Palavras-chave: *Cybersecurity, passwords, hackers, segurança.*

Abstract: *The problem of simplifying passwords. The dangers of repeating the same password on multiple systems. Analysis of the main methods used by hackers to gain access to personal information. Solutions for password security. Secure Passwords*

Keywords: *Cybersecurity, passwords, hackers, security.*

I. Introdução

Pretende-se com este artigo refletir sobre Cybersecurity, propor boas práticas e soluções para a criação, utilização e manutenção de passwords a fim de se manter o maior nível de segurança possível.

Serão explicitadas as principais técnicas de Hacking contra passwords, será dado enfoque à questão da proteção de passwords aplicadas a correio eletrónico. Descrevem-se os sistemas relevantes para a gestão e proteção de passwords. Indica-se um conjunto de possibilidades para a criação de passwords fortes. Será abordada a questão 2FA e MFA. Por fim, serão analisadas as questões relativas à segurança das passwords implementadas em telemóveis.

II. Questões de segurança nas passwords

Muitas pessoas consideram as passwords algo aborrecido, e simplificam-nas sempre que lhes é possível. A desvalorização do papel das passwords é comum mesmo por dirigentes de topo nas organizações. Quer por falta de informação quer por puro laxismo.

Provavelmente, o resultado destes comportamentos é prejudicial.

As passwords são a primeira linha de defesa em relação a quase todos os sistemas de informação, e em alguns casos a única defesa contra intrusão e tentativa de roubo de dados ou informação, tanto na vida pessoal como na vida profissional.

Existem variadíssimos métodos para quebrar as contas e as passwords, sendo que o mais utilizado é o adivinhar passwords fracas (exemplo: data de nascimento, numerais

seguidos, do tipo 123456, nomes próprios, do tipo pedrobrandao, etc.). Outro método muito utilizado é o da reutilização. Ou seja, um hacker consegue quebrar uma password fraca, e de seguida tenta utilizá-la noutros sistemas, ou tenta utilizá-la com pequenas variações, caso ela não funcione na sua versão original. Isto porque sabemos que a grande maioria das pessoas utiliza a mesma password em todos os sistemas (telemóvel, home banking, Facebook, Twitter, computador no trabalho, etc). Até porque, hoje em dia, é difícil encontrar um sistema que não necessite de uma password.

As passwords são uma combinação de caracteres que autenticam a identidade do utilizador. Tecnicamente confirmam que alguém que diz ser XYZ é efetivamente XYZ.

III. "Cracking" da password

Antes de se analisar a criação de passwords seguras, é aconselhável conhecerem-se os principais métodos utilizados por Hackers para quebrarem passwords. O "Cracking" de passwords é muito mais fácil do que a maioria das pessoas pode imaginar, ou sabe. Este método ou processo consiste em decifrar passwords a fim de se obter um acesso indevido a um sistema. Muitas vezes este método não recorre a ferramentas sofisticadas, ou mesmo a programas em computadores.

Um sistema simples e que não é ilegal de "password attack" denomina-se de "dumpster diving", consiste em vasculhar o seu lixo à procura de um qualquer documento que inadvertidamente tenha a password escrita. É por isso que a primeira regra de ouro em termos de segurança de passwords é nunca, em caso algum, serem escritas, independentemente do suporte.

Explicito alguns dos mais importantes tipos de ataques (mantêm-se as expressões em inglês):

- "Dictionary Attack": é a técnica mais comum utilizada para descobrir a password. Trata-se de um tipo de ataque rápido, um ficheiro de texto com centenas de palavras de dicionário executado por um software de "cracking" contra plataformas de login de um determinado utilizador, até que uma das palavras do dicionário seja a password desse utilizador. Estas listas por norma contêm milhões de expressões. É uma ferramenta extremamente eficaz.

- "Hybrid Attack": um software de "cracking" usa listas de passwords roubadas, mas eventualmente já alteradas pelos seus utilizadores, acrescentando-lhe sucessivamente símbolos e letras. Esta técnica baseia-se no facto de que a maioria das pessoas ao alterarem as suas passwords utilizam a anterior acrescentando-lhes uma letra ou um símbolo. Por exemplo, adicionar um número a uma password prévia é uma prática comum.

- "Brute Force Attack": este é um dos mais completos tipo de ataque. Baseia-se na verificação sucessiva da viabilidade de combinações. Começando com "A", "B", (…) até se encontrar a combinação correta.

Algumas vezes os Hackers têm acesso a "Hashed passwords", em que a password está encriptada, através de funções unidirecionais. A única forma de nos protegermos contra ataques deste tipo é criarmos passwords o mais longas possíveis, para que o tempo necessário para a quebrar não seja viável e útil ao hacker. O mínimo aconselhável são dezasseis caracteres para a criação de uma password. Para se ter uma ideia do tempo necessário para a decrifração de uma password, com a tecnologia existente hoje, e sem recurso a computadores quânticos, podemos considerar a necessidade de um milénio para acertar na combinação de uma password com trinta e dois caracteres. Por isto, desaconselha-se fortemente o uso de passwords com quatro caracteres.

IV. Importância da password no correio eletrónico

A principal razão pela qual a password do correio eletrónico se reveste de importância acrescida é o facto, por norma, de esta ser utilizada noutros sistemas, e ainda porque o correio eletrónico é utilizado frequentemente para o envio de atualizações de passwords. Logo, quem conseguir quebrar a password de um sistema de correio eletrónico tem grandes probabilidades de aceder a outras passwords.

A melhor forma de evitar este problema é a utilização da autenticação em dois fatores, assim maximiza-se a proteção no acesso à conta de correio eletrónico. Grande parte dos serviços e programas de correio eletrónico já dispõem dos sistemas 2FA bastando ir às configurações na área de segurança ou privacidade e ativar este tipo de autenticação.

IV – Criação de passwords fortes

Não se devem utilizar palavras comuns na criação de passwords. Por exemplo, evitar a utilização de palavras do dicionário, palavras escritas ao contrário, números sequenciais. Não se devem utilizar palavras relacionadas com informação pessoal. Não utilizar em passwords nome próprio, data de nascimento, localidade onde habita, número de telefone, etc.

As passwords fortes são criadas considerando dois princípios: o comprimento da password e a entropia.

O comprimento está relacionado diretamente com o número de carateres, quanto maior for o seu comprimento, mais segura é a password.

A entropia é a medida da aleatoriedade da password. Quanto maior for a entropia maior é a segurança. Por exemplo, peça a oito amigos que indiquem uma letra do alfabeto de forma aleatória, depois componha a password com as oito letras. Esta password tem uma elevada entropia. Outro exemplo, utilize um programa informático para criar aleatoriamente uma password de dezasseis carateres. Neste caso a entropia é ainda maior, logo o nível de segurança muito superior.

V – Passwords em dispositivos móveis

A perda de dispositivos móveis é extremamente comum. Hoje os dispositivos móveis estão pejados de informação do proprietário e em alguns casos das empresas onde os proprietários do dispositivo trabalham. Como passwords, contactos, pin de cartões de crédito, contas bancárias, texto e fotografias. Esta informação tem de estar protegida caso o dispositivo seja roubado ou perdido.

Para que o dispositivo móvel tenha um mínimo de segurança implementada, devemos considerar os seguintes procedimentos:

a) Usar uma password para bloquear o ecrã. Esta é a primeira linha de defesa. Normalmente é um PIN com numerais.
b) Utilizar uma aplicação do tipo "*Find my Phone*". Permitem a localização do dispositivo, em alguns casos permitem o controlo remoto do mesmo. Alguns dispositivos já vêm com um sistema de segurança que em caso de várias tentativas mal sucessivas de login toda a informação é autodestruída. Este sistema deve estar configurado e ativo.
c) Colocar um autocolante permanente na parte de trás do dispositivo com o seu email. Se for um mero caso de ter esquecido o telemóvel em determinado local quem o encontrar pode contactá-lo por email.
d) Faça um back-up frequente de todos os seus dados do telemóvel para um sistema de *cloud computing*. Em caso de perde definitiva pode automaticamente fazer o download dos dados para um novo dispositivo.
e) Mude com frequência a sua password de acesso ao telemóvel.
f) Se o dispositivo dispuser de aplicações que permitem ter passwords, como por exemplo o *Telegram*, implemente nessas aplicações uma password forte, está a criar mais uma camada de segurança.
g) Sempre que possível não guarde informação sensível ou de trabalho no telemóvel armazene-a num sistema de *cloud computing*. Por exemplo pode configurar o telemóvel para que após ter tirado uma foto a armazene em *cloud computing* e nunca no cartão local.
h) Nunca escreva num papel as passwords.

VII. Conclusão

A segurança das passwords é extremamente importante e protege a informação pessoal ou

empresarial. É a primeira linha de defesa contra ataques de hackers.

Utilize sempre que possível um sistema de autenticação por dois fatores.

Utilize um programa informático para gerar passwords, assim consegue um elevado nível de entropia.

Use uma password para cada serviço, não use a mesma password para diversos serviços ou sistemas.

Assegure-se de cada password tem no mínimo dezasseis carateres.

Não crie passwords com informação pessoal.

Nunca escreva em lado algum as passwords.

Não partilhe as passwords nem com os seus amigos e familiares.

Nunca utilize respostas verdadeiras e reais a perguntas de verificação em sistemas dessegurança. Invente as respostas.

Nunca envie informação de acesso a sistemas ou passwords via correio eletrónico.

XIV. Bibliografia

Diogenes, Yuri (2028). Cybersecurity - Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt.

Stallings, William (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley.

Maymi, Fernando (2018). CompTIA CySA+ Cybersecurity Analyst Certification. CompTIA.

Hubbard, Douglas (2018). How to Measure Anything in Cybersecurity Risk. Wiley.

Kohnke, Anne (2018). Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework. CRC Press.

Behan, Maria (2018). Beginner's Guide to Information Security: Kickstart your security career with insight from InfoSec experts. Peerlyst.

Brooks, Charles (2018). Cybersecurity Essentials. Sybex.

Arnold, Rob (2017). Cybersecurity. Threat Sketch, LLC.

Kohnke, Anne (2016). The Complete Guide to Cybersecurity Risks and Controls. CRC Press.

Guiora, Amos (2017). Cybersecurity: Geopolitics, Law, and Policy. Routledge.