Vše začíná a končí u hesla

autor prezentace: Tomáš Hamberger

KLUB AKTIVNÍCH VE VZDĚLÁVÁNÍ

eSafety Label for a safer school

AGENTURA PRO ROZVOJ BROUMOVSKA

Teplice nad Metují

Heslo kam a jak?

- Heslo je prostředek k ověření totožnosti.
- Každá aplikace si ukládá naše hesla – měla by si je ukládat hashovaná do své databáze.
- Do určité míry dosud nemáme 100% kontrolu nad svými hesly – úniky dat ze špatně zabezpečených serverů, apod.
- Stále je v ČR mnoho organizací, e-shopů, ze kterých se dá volně stáhnout databáze s uživatelskými jmény a hesly, protože používají nedostatečné nebo zastaralé hashování.

Úniky dat aneb jak je to jednoduché

- Existuje volně přístupný web, na kterém jsou anonymně publikovány rozsáhlé úniky dat.
- Tento web má samozřejmě fultextový vyhledávač, takže stačí zadat výraz CZ., a zobrazí se vám úniky, které obsahují české emailové adresy.
- Není výjimkou najít emaily i s jejich hesly.

Úniky dat aneb jak je to jednoduché

Cracking / lámání

- Slovníkový útok - Místo všech možných kombinací zkoušíme jen slova, která jsou uvedená v nějakém seznamu nebo slovníku, protože uživatelé taková slova znají a tedy často používají jako hesla.
- Kombinatorický útok – jména.text + příjmení.text – (seznam jmen a příjmení na stránkách MV ČR)
- Většina hesel je vytvořena předvídatelně, viz algoritmy.
- V současnosti se nejvíce na lámání hesel používají výkonné grafické karty.
- Aktuálně nejvýkonnější, běžně dostupná karta, dokáže vypočítat 31 miliard hashů za vteřinu.

Jak to tedy je s lámáním hesla?

Potřebuji program na lámání hesel – John the Ripper, HashCat.

Potřebuji zdroj – online slovníky, seznamy již uniknutých hesel, apod.

Potřebuji výkonnou grafickou kartu.

Zasazení do kontextu

- Počet všech možných kombinací pro heslo složené z 8 znaků, které mohou být malé písmeno, velké písmeno nebo číslo je 218 bilionů. Vygenerovat tolik hashů zabere kartě GTX 1080 přibližně 2 hodiny, přesněji 7043 vteřin.
- Projít všechny kombinace hesla o devíti znacích složeného z malých a velkých písmen a čísel zabere 62× tolik času, tedy cca. 5 dní.
- Desetiznakové heslo složené z malých a velkých písmen a čísel má 62^{10} možných kombinací. Vygenerovat tolik hashů zvládne GTX 1080 za 313 dní.
- Kombinací hesla dlouhého 12 znaků by karta potřebovala asi 3 300 let.

Co z toho plyne?

- Heslo by mělo mít minimálně 12 znaků.
- Heslo by měl být nejlépe náhodně vygenerovaný, abstraktní pojem.
- Heslo by mělo být dlouhé, unikátní a náhodné.
- Co účet – to heslo!
- Používat dvoufaktorovou autentizaci (2FA).
- Dvoufaktorové ověřování nabízí – google, facebook, twitter, alza nebo slevomat.
- Pozor na recyklaci hesla.
- Využívejte PASSWORD MANAGER – KEE PASS, LAST PASS, apod.

Ideální heslo

- /F-PjxTa-@Sw1´JJ/U 85uk+Kj

Příklady z praxe

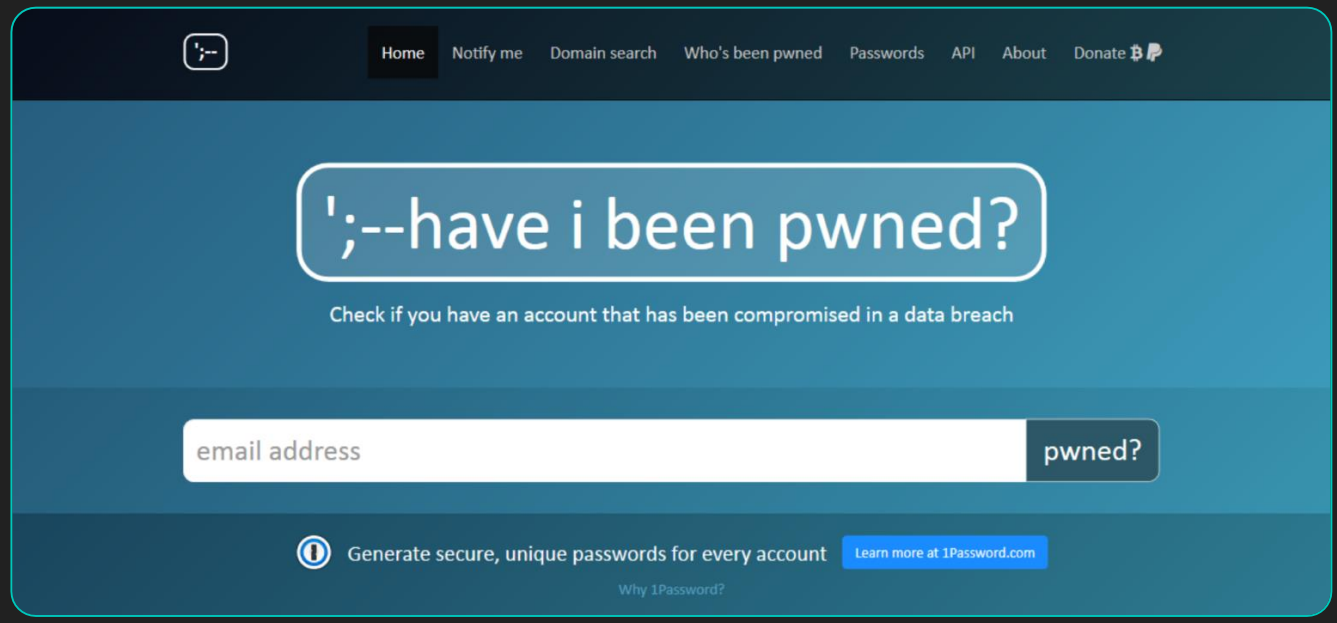
- Konkrétně Internet Mall, a.s. nezabezpečil osobní údaje nejméně 735 956 zákazníků v rozsahu jméno, příjmení, e-mailová adresa, heslo uživatelského účtu, případně telefon před neoprávněným přístupem v období minimálně od 31. prosince 2014 do srpna 2017. V důsledku toho došlo v době od 27. července do 25. srpna 2017 ke zpřístupnění uvedených osobních údajů na serveru Uložto.cz

Příklady z praxe

- Únik dat ze společnosti T – Mobile. (2016)
- Co uniklo: jméno, příjmení, datum narození, adresa, telefonní číslo, kód zákazníka, tarif, značka zařízení, údaj o průměrné útratě, číslo účtu a kód banky (pokud byla zřízena inkasní platba).
- Jednalo se o data 1,2 milionů zákazníků.
- Pachatel byl zaměstnanec firmy, který data nabízel k prodeji třetím stranám.

Mám zlomený účet?

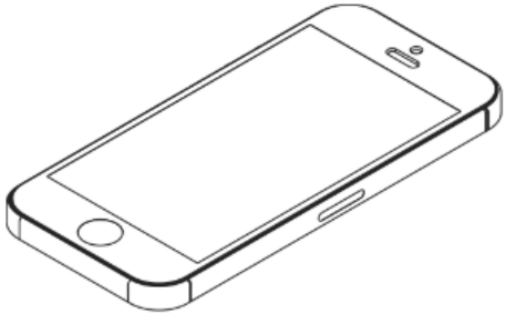
- Na Have I Been Pwned? si můžete ověřit, jestli vaše e-mailová adresa (nebo adresa kohokoliv jiného) nebyla v nějakém veřejně známém úniku dat. Troy Hunt, provozovatel této služby, do ní nahrává data, která najde veřejně na webu nebo která mu někdo poskytne. Slovo „pwned“ pochází z „owned“, obojí vyjadřuje *přivlastnění* něčeho, v tomto případě vaší online identity.



Shrnutí pro školní prostředí

1. Bezpečné heslo (zejména pro školní databázi a nezapomínat na účetnictví)
2. Aktuální hrozbu představuje KEYLOGGER (případy napadnutí systému Bakaláři a změn klasifikace)
3. Falešná wi-fi (stejný nebo podobný název, stejné heslo) velice těžké rozpoznat!

Mentimeter – zpětná vazba v reálném čase



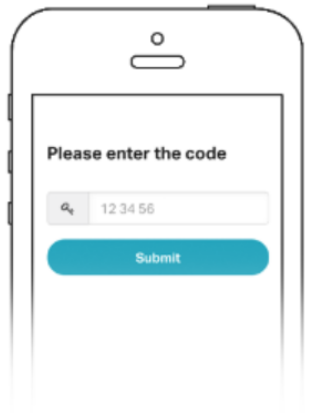
1

Grab your phone

www.menti.com

2

Go to www.menti.com



3

Enter the code 59 65 83 and vote!

Děkuji za Vaši pozornost.

KLUB AKTIVNÍCH VE VZDĚLÁVÁNÍ

Teplice nad Metují

AGENTURA PRO ROZVOJ BROUMOVSKA

eSafety Label for a safer school

Cílem této přednášky je upozornit na potřebu kybernetického vzdělávání a ochranu obyvatel ČR. ©TH