COLONNADE
A FAIRFAX COMPANY

Kybernetické útoky a slabá hesla

12/5/2025

Colonnade Confidential

Kybernetické útoky

Statistiky 2024

Průměrná cena úniku dat: 4,88 milionu USD

Řešení incidentů s hesly trvá v průměru 88 dní

30 % **uživatelů zažilo útok kvůli slabému heslu**

66 % **lidí používá stejné heslo na více účtech**

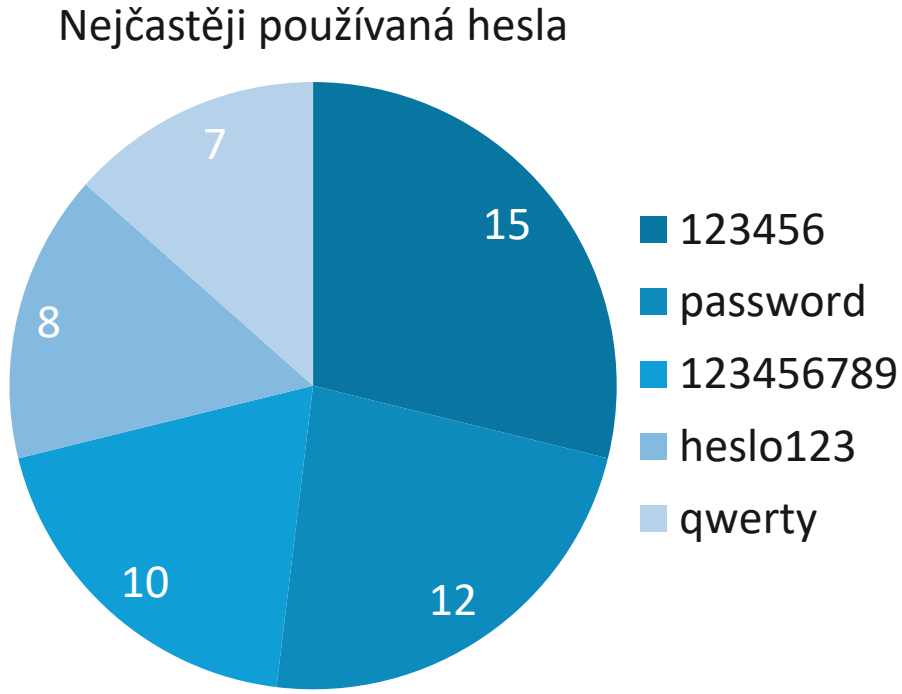
194 dní **=doba detekce úniku**

Colonnade Confidentia

Kybernetické útoky

Významné incidenty 2023-2024

- RockYou2024: 10 miliard uniklých hesel
- 23andMe: únik genetických dat 5,5 milionu lidí
- Ticketmaster: postiženo 560 milionů zákazníků



Colonnade Confidential

Kybernetické útoky

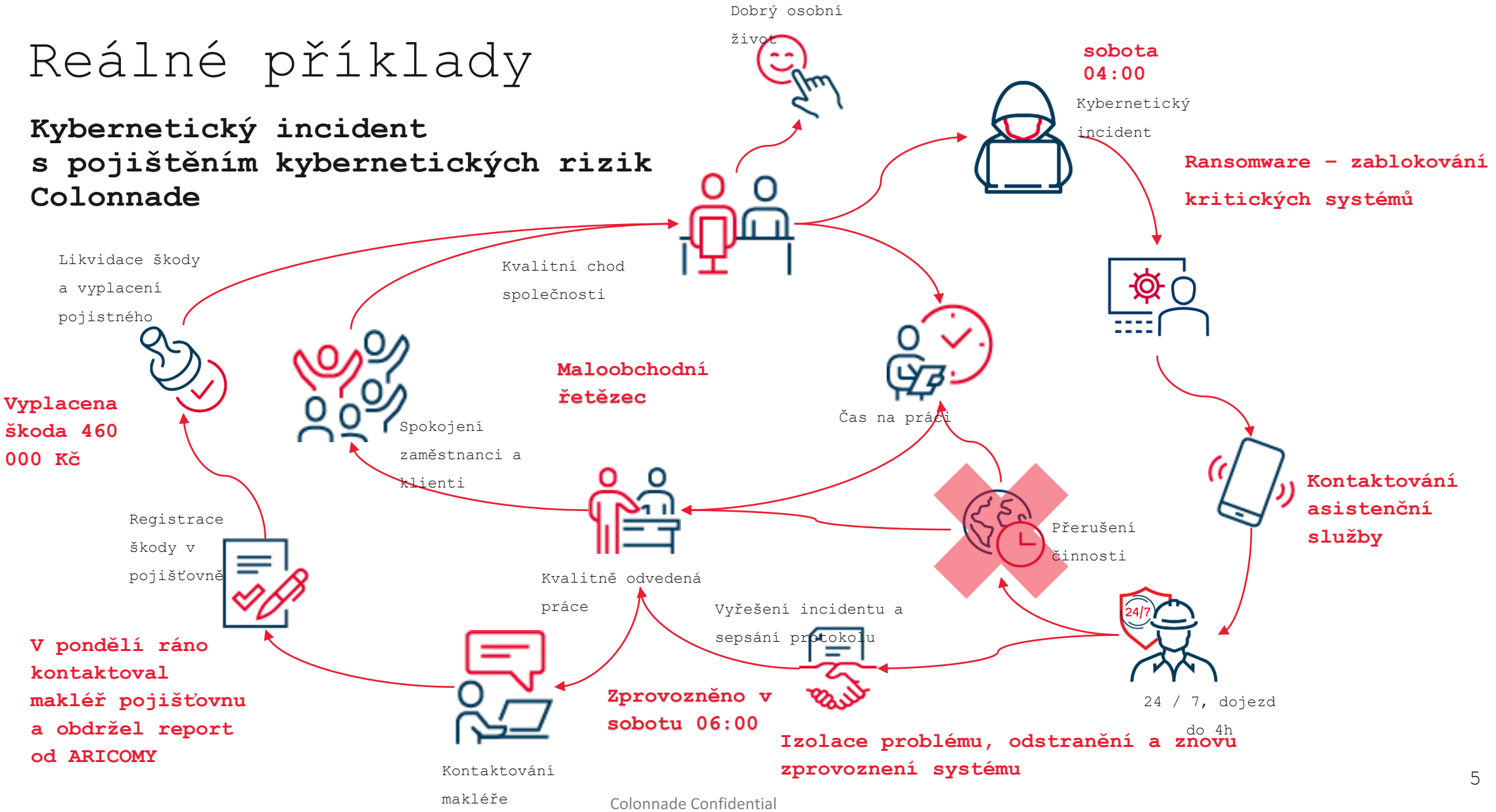
Příklady

- **Únik dat u České pošty (2020)**
  Útočníci získali přístup k e-mailovým adresám, telefonním číslům a dalším osobním údajům. Mohl být důsledkem slabé ochrany hesel u některých interních systémů.
- **Únik dat u Sazka (2021)**
  Na internet byla zveřejněna databáze obsahující citlivé údaje milionů zákazníků Sazky. Únik mohl být výsledkem prolomení šifrování nebo jiného typu útoku. Mnozí uživatelé si pak museli změnit hesla.
- **Únik hesel u Seznam.cz (2019)**
  Seznam.cz čelil úniku přihlašovacích údajů na některých z jejich internetových služeb. Důsledkem bylo zneužití slabých hesel, která byla odhadnutelná a nechráněná silnými metodami šifrování.
- **Únik dat u VZP (Všeobecná zdravotní pojišťovna, 2021)**
  Útočníci získali jména, rodná čísla a pojišťovací čísla. I když se v tomto případě nejednalo o přímý únik hesel, jedná se o případ, kde byly citlivé údaje použity k podvodům a dalším bezpečnostním problémům. Únik mohl být způsoben slabou správou přihlašovacích údajů a přístupu.
- **Únik dat u České spořitelny (2018)**
  Útočníci získali přístup k přihlašovacím údajům na webových stránkách banky. I když banka tvrdila, že šlo o útok na třetí stranu, tento incident vedl k nutnosti změny přihlašovacích údajů pro velkou část klientů.
- **Únik dat u aplikace Twisto (2021)**
  Únik zahrnoval osobní údaje a přihlašovací údaje uživatelů. Tento incident podtrhl význam silného zabezpečení aplikací a používání silných hesel pro prevenci úniků.

Colonnade Confidential

Reálné příklady

Kybernetický incident s pojištěním kybernetických rizik Colonnade



ÚNIK DAT

NÁKLADY NA OBNOVU

ÚNIK DAT A ZVEŘEJNĚNÍ 117 000 OSOBNÍCH ÚDAJŮ STUDENTŮ

Následuje:

- náklady na IT experty za účelem zjištění příčiny útoku a přesného počtu zveřejněných údajů
- náklady na oznámení (informační dopis všem studentům a zřízenícall centra)
- náklady na PR
- pokuta udělená dozorovým orgánem za zveřejnění citlivých informací

Celková škoda: 2 000 000 ,- Kč

Colonnade Confidential

VÝPADEK SÍTĚ

ÚTOK HACKERŮ NA IT INFASTRUKTURU – cestovní ruch

- zašifrování IT systému klienta – ČT v odp. hodinách
- okamžité zablokování všech PC = přerušení on line prodeje služeb a zboží
- ČT večer – kontakt assistenční služby, odmítnutí ze strany kleinta ve snaze řešit pomocí svých vlastních prostředků/ IT podpory
- PA – opětovné kontaktování asistenční služby, okamžitá podpora = SO zprovoznění všech krytických systémů

- snížení zisku pojištěného v důsledku nemožnosti prodávat služby a zboží
- náklady na IT experty za účelem zjištění příčiny výpadku systémů

Celková škoda: 5 000 000 ,- Kč vs. původní odhad cca 25 000 000,-

Colonnade Confidential

RANSOMWARE

HACKERSKÝ ÚTOK RANSOMWARE

zašifrování IT sítě, požadované výkupné; Společnost se stala terčem kybernetického útoku, což vyžádalo náklady obnovu IT Systému.

Dne 6. 9. 2022 v brzkých ranních hodinách začal útok typu ransomware. Kolem 7:50 si ho všiml administrátor a začal sérii kroků vedoucí k ohraničení útoku a záchraně dosud nezašifrovaných dat. V 9:30 dorazili zástupci přivolaného bezpečnostně-forenzního týmu a pomohli administrátorovi izolovat útok. Dostali situaci pod kontrolu, zjistili rozsah škod = téměř všechny běžící uživatelské stanice a některé servery byl zašifrovány s koncovkou .UATHN a byl vedle nich návod jak kontaktovat útočníka a zaplatit mu výkupné za rozšifrování. S pomocí přivolaného týmu jsme postupně infrastrukturu obnovili bez pomoci útočníka.

Celková škoda cca 300 000 ,- Kč

Colonnade Confidential

Doporučení

- Používat silná a unikátní hesla
- Aktivovat dvoufaktorové ověření (2FA)
- Vyhnout se osobním údajům v heslech
- Používat správce hesel
- Kontrolovat úniky přes HaveIBeenPwned.com
- Častěji měnit hesla
  - každé 3 měsíce pro systémy obsahující citlivé informace
  - 1 ročně u běžných účtů
  - nepoužívat 1 heslo pro všechno

Colonnade Confidential

Děkuji za pozornost.

Colonnade Confidential