AUXILIUM
Cyber Security

# Penetrační testy digitální infrastruktury

# Kdo jsem a co děláme?

- Vystudoval jsem kybernetickou bezpečnost na TU Berlín
- První praxe v Auxilium Cyber Security (Karlsruhe)
- Od roku 2019 vedu naší kancelář v Praze
- Pražská kancelář se specializuje na penetrační testy:
  - Vestavné systémy
  - Webové aplikace
  - Mobilní a desktopové aplikace
  - API
  - Podniková infrastruktura
- **Co je ten penetrační test?**

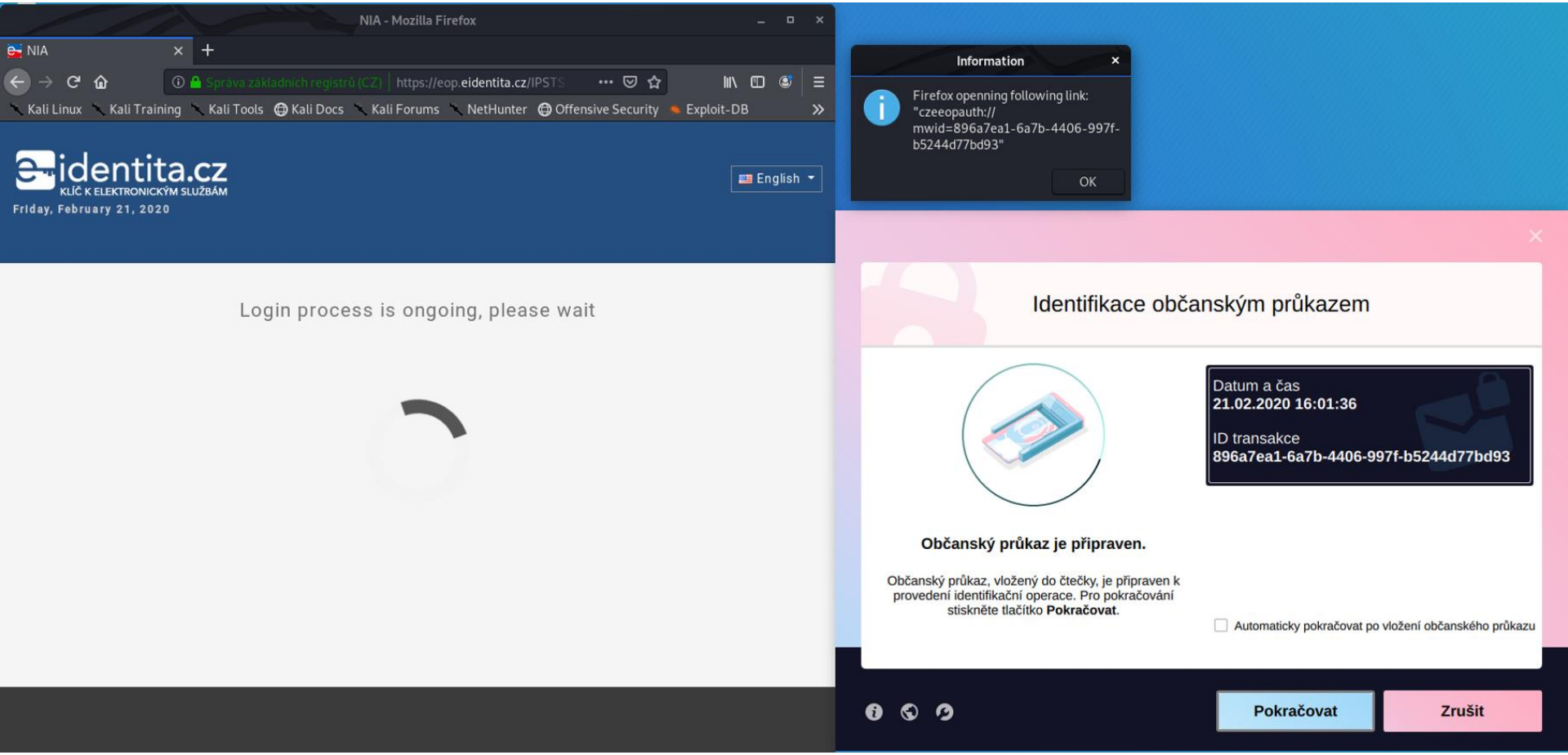
**Penetrační test** je metoda hodnocení zabezpečení počítačových systémů, která se provádí simulací reálného útoku na tento systém.

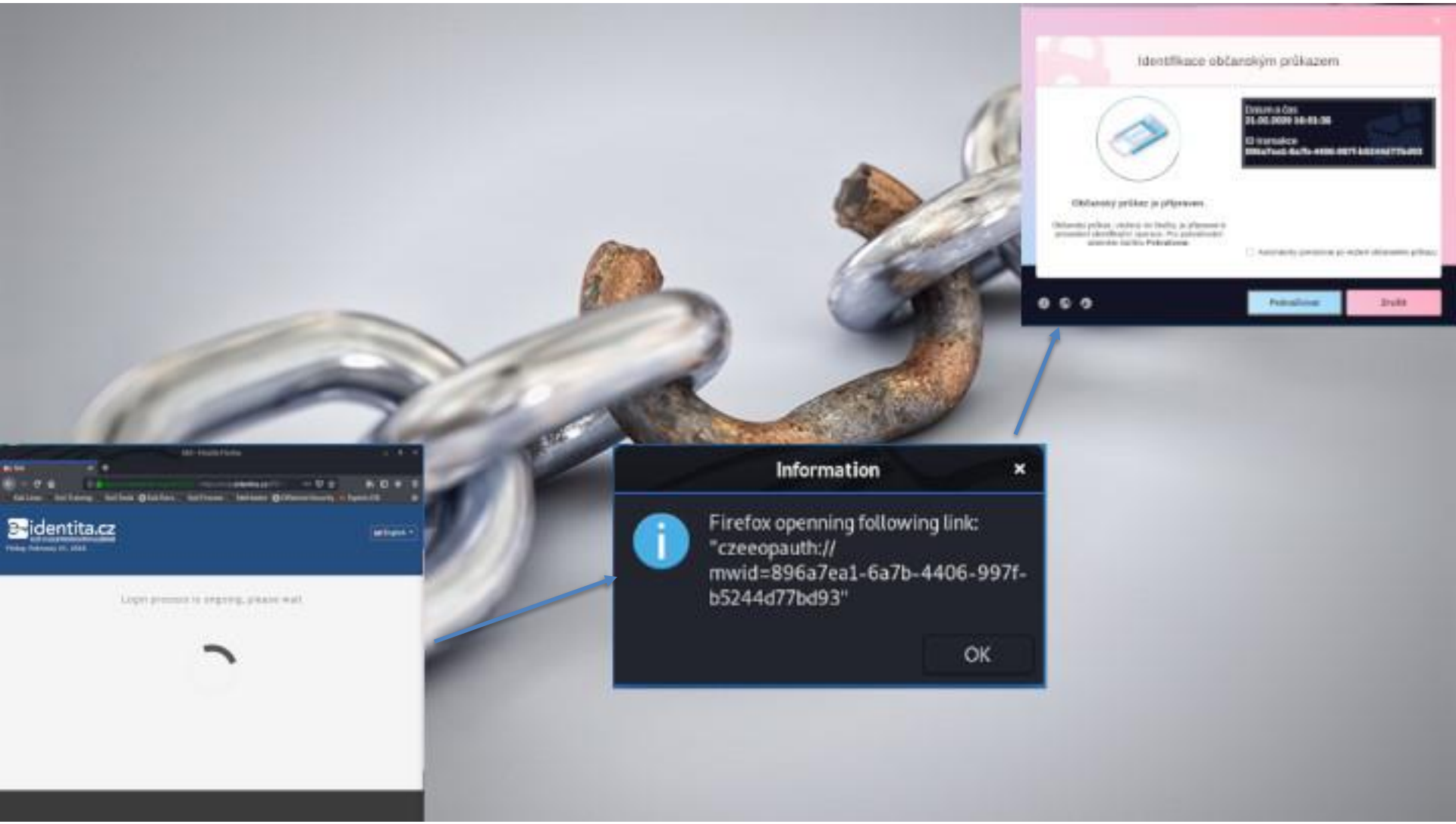
# Kde bude obvykle prolomena kybernetická bezpečnost?

# Řetěz je jen tak silný jako jeho nejslabší článek

- Platí dvojnásob v kybernetické bezpečnosti
- Skvělá podniková infrastruktura, ale…
  - …jednofaktorová autentizace na VPN
- Bezpečnou aplikaci A a aplikaci B, ale…
  - …jejich integrace není optimální
- Dovolte mi demonstrovat na případu eObčanky
- Zveřejněno v angličtině na konferenci QuBIT
- QuBIT 2020: Virus Harvesting Czech eObčanka (eID Card) Identities

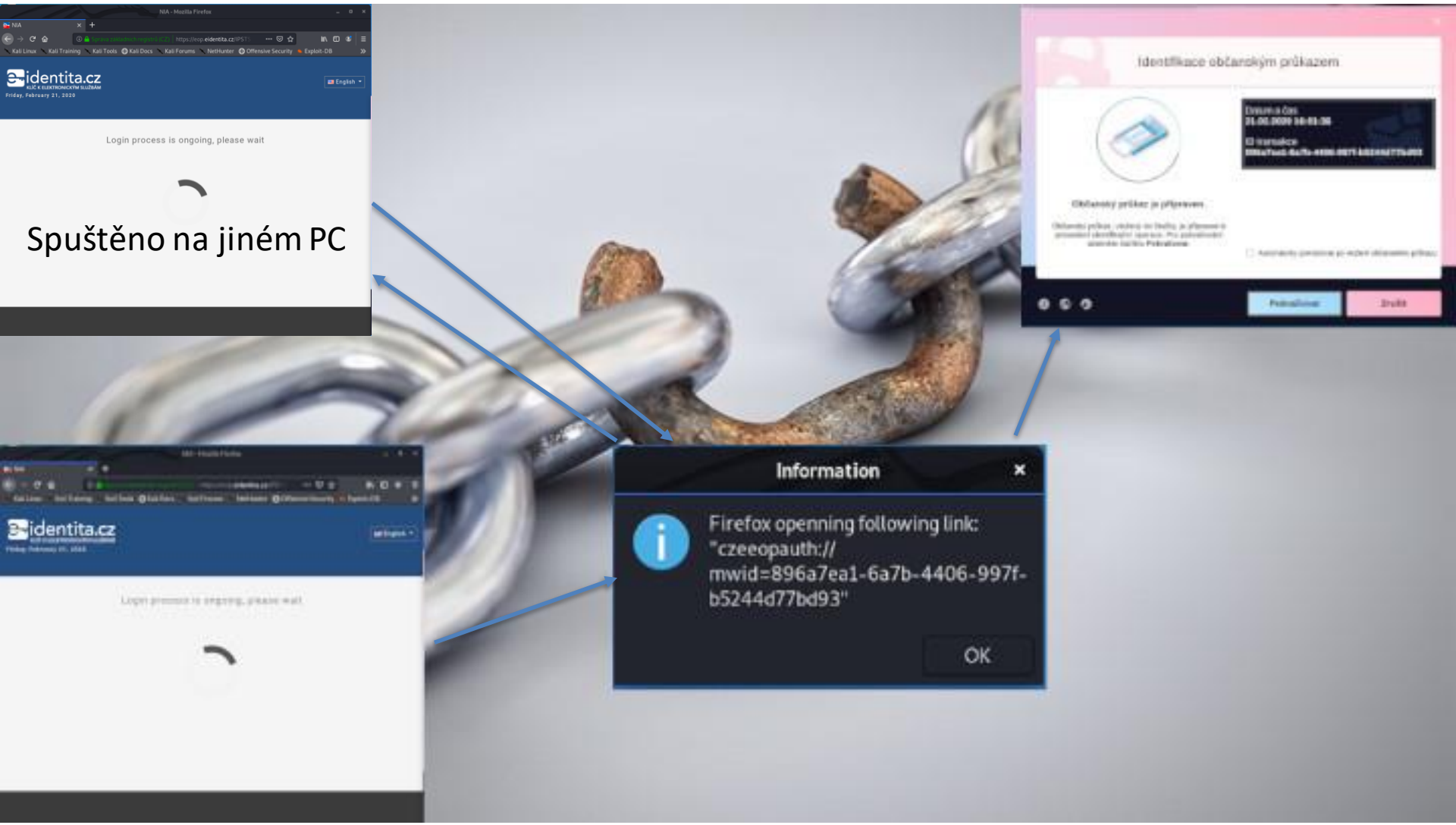
# Proces přihlášení eObčankou (2019)





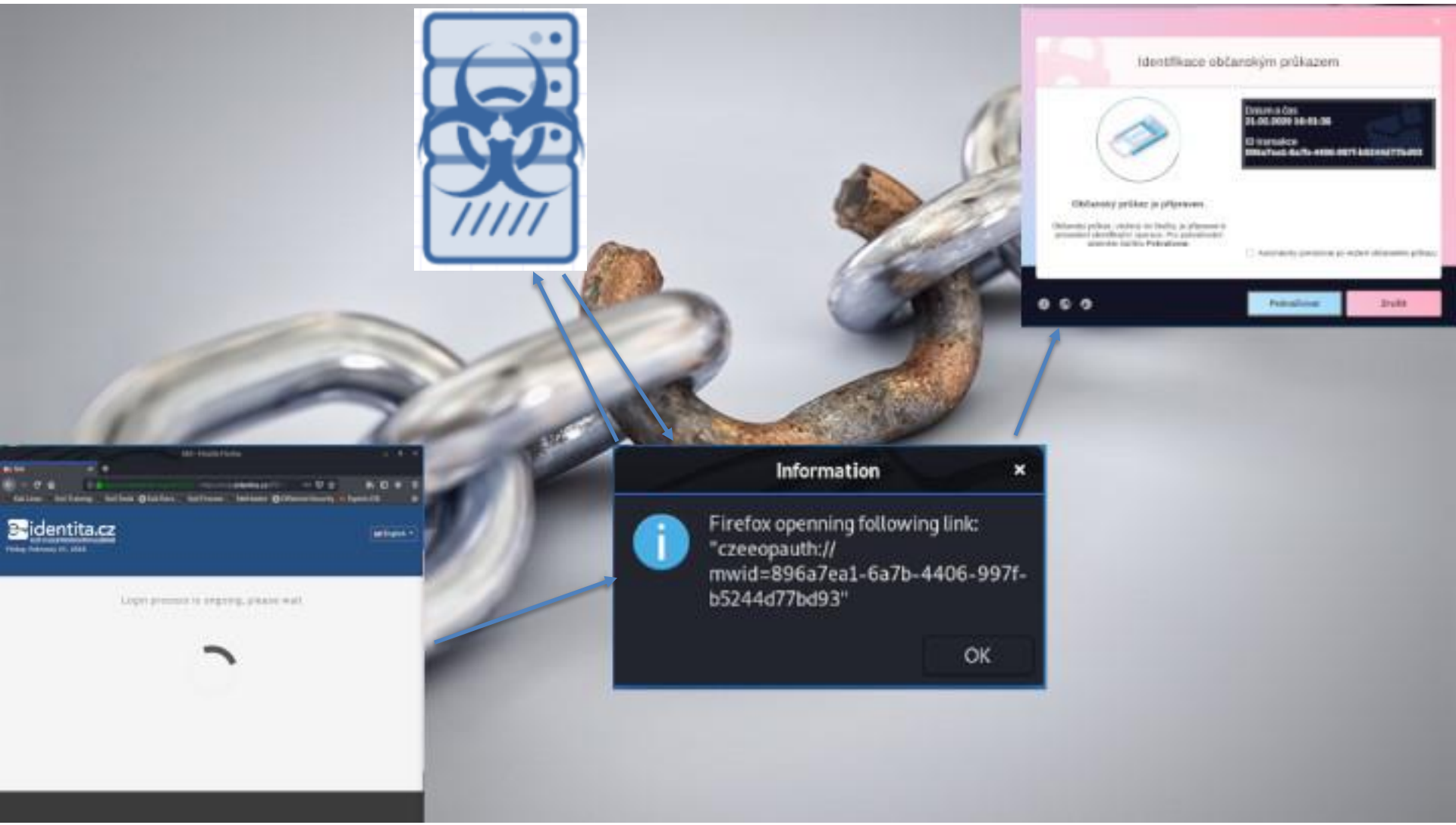
# Řetěz přihlášení eObčankou

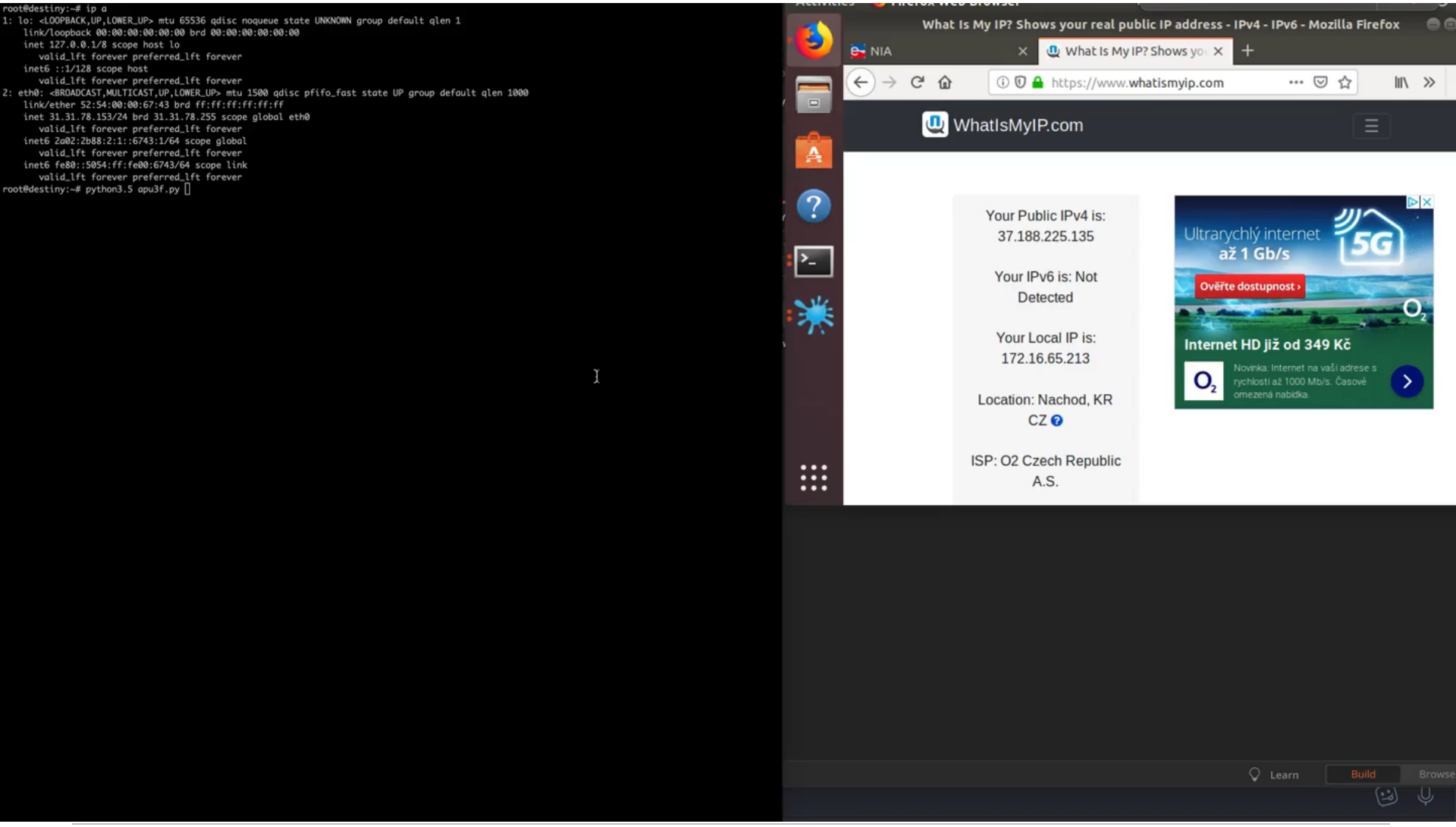
- Aplikace A: webová aplikace eidentita.cz (SSO)
- Aplikace B: eObčanka – Identifikace (komunikace s eOP)
- Obě aplikace velmi solidně vyvinuty
- Bohužel A předává B ID transakce přes nezabezpečený odkaz
- **Co se stane pokud toto ID bude „změněno“?**
- Uživatel jistě nic nepozná, jelikož ID transakce se nezobrazuje v A
- Vidí jej pouze v aplikaci B



# Narušený řetěz přihlášení eObčankou

- Útok lze bohužel plně automatizovat
- Pro demonstraci útoku jsme vyvinuli 2 komponenty:
  1. Virus, který běží na PC kde se přihlašuje občan
  2. Webovou službu, která běží v cloudu
- V okamžiku spuštění aplikace B je volání zachyceno virem
- Webová služba vygeneruje nové přihlašovací ID a předá jej viru
- Vir změní přihlašovací ID uživatele za ID útočníka
- Nic netušící občan dokončí přihlášení zadáním PINu
- Útočník bude přihlášen jménem občana
- Občanův přihlašovací pokus neuspěje (timeout)



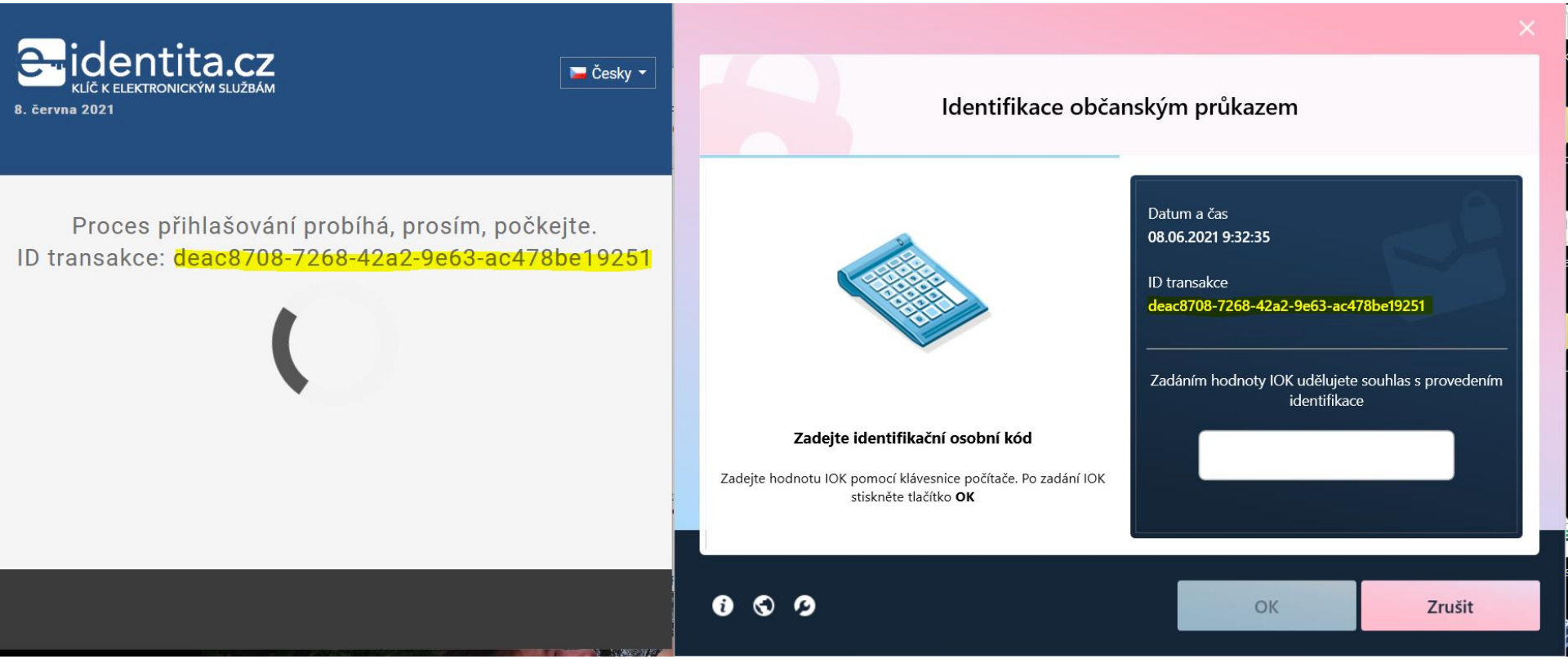


# Proč se jedná o bezpečnostní riziko?

- Předpokladem je přihlašovací pokus ze „zavirovaného“ PC.
- Nedá se předpokládat, že by se útok vyplatil kvůli 1 oběti.
- Adopce eObčanky bude nejspíše do budoucna stoupat.
- Masové rozšíření viru tak může být výhledově zajímavé:

1. Ekonomická motivace
    - Daňové vratky (daňový portál, ePortál ČSSZ)
    - Přístup k lékům na předpis (eRecept)
2. Politická motivace
    - Ovlivnění či znevěrohodnění potenciálních online voleb

# Co je reálným výstupem tohoto nálezu?



# Shrnutí penetračních testů

- Řetěz kybernetické obrany je jen tak silný jako jeho nejslabší článek
- Penetrační testování je o odhalování těchto slabých článků
- Penetrační test = den, týden, měsíc dlouhý útok na…
  - …podnikovou infrastrukturu
  - …aplikaci (web, API, mobil, desktop)
  - …produkt (hlavní jednotka auta, domácí alarm, IoT)
- Výstupem je report a prezentace slabých článků (zranitelností)
- Technický přínos = robustnější produkt / infrastruktura
- Business přínos = útočník při stejném úsilí neuspěje (útok se nevyplatí)

# Děkuji za pozornost

Auxilium Cyber Security

martin.pozdena@auxiliumcybersec.cz

+420 739 467 470