AUXILIUM
Cyber Security

Penetrační testy jako nedílná součást strategie informační bezpečnosti

Kdo z Vás pravidelně využívá penetrační testy?

Penetrační test je metoda hodnocení zabezpečení počítačových systémů, která se provádí simulací možných útoků na tento systém.

K čemu je to vlastně dobré? – 1

- **Může jedna zranitelnost či kliknutí „vymazat“ ICT organizace?**

ČT 24

KORONAVIRUS | SLOVENSKÉ VOLBY | DOMÁCÍ | SVĚT | REGIONY | EKONOMIKA | KULTURA

Hackeři ochromili benešovskou nemocnici. Nelze spouštět přístroje, ruší se operace

AKTUALIZOVÁNO 11. 12. 2019

Provoz Nemocnice Rudolfa a Stefanie Benešov ochromil kryptovirus, který v noci na středu napadl její počítačový systém. Nelze spustit žádný přístroj, všechny plánované operace jsou zrušené. Zdravotnické zařízení využilo nabídky pomoci odborníků z Národního úřadu pro kybernetickou bezpečnost. Podle ředitele nemocnice se určitě nepodaří plný provoz obnovit během středečního dne, problémy teoreticky mohou trvat i týdny.

Maersk had to reinstall all IT systems after NotPetya infection

By Ry Crozier
Jan 25 2018
10:30AM

16 Comments

"4000 new servers, 45,000 new PCs, 2500 applications".

Shipping giant Maersk was forced to reinstall its entire IT environment in 10 days to recover from the NotPetya malware in June last year.

Chairman of AP Moller-Maersk, Jim Hagemann Snabe, revealed the full extent of damage caused by the infection while speaking at the World Economic Forum in

NotPetya incident v Maersku

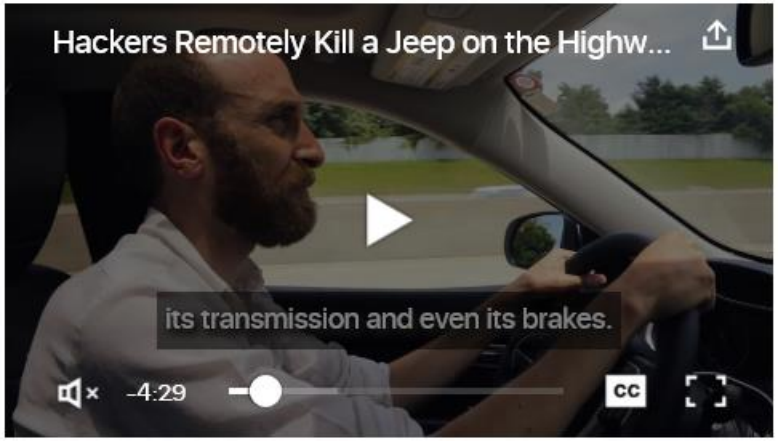
- Infrastruktura postavená na Microsoftu
- SMB zranitelnost **EternalBlue** (CVE-2017-0144)
- Patch zveřejněn v březnu 2017
- Útok NotPetya proběhl na konci června 2017
- Maersk přišel o 4000 serverů, 45000 PC a 2000 aplikací
- Infrastrukturu se podařilo obnovit za 10 dní
- Za cenu 250-300 milionů dolarů – 5-6 miliard korun
- **Obdobná zranitelnost BlueKeep z května 2019** (CVE-2019-0708)
- **A opět EternalDarkness z března 2020…** (CVE-2020-0796)

- https://www.youtube.com/watch?v=VaqIYlYmDbA

K čemu je to vlastně dobré? – 2

- **Může špatný bezpečnostní návrh Vašeho produktu způsobit autonehodu?**

Hackers Remotely Kill a Jeep on the Highway—With Me in It



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Jeep Cherokee 2014 Hack

- Hlavní jednotka (chytré autorádio) trvale připojeno do Internetu
- Chybně navržená a neotestovaná infrastruktura
- Umožnila vzdálenému útočníkovi převzít plnou kontrolu nad autem
- Útočník byl schopen vzdáleně ovládat:
  - Veškeré řízení: brzdy, řazení, zatáčení, motor
  - Rádio, klimatizaci
  - Ostřikovače, stěrače atd

- Video a článek na: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Jak efektivně využít penetrační test?

- Absolutně bezpečný systém mimo akademickou sféru **neexistuje**
- Bezpečnost je vždy funkce **motivace (útočník)** vs **investice (obránce)**
- Motivace útočníka:
  - Finanční (kybernetický zločin jako ransomware, bankovní trojan)
  - Politická (součást konfliktu, aktivismus atd)
  - Nekalé obchodní praktiky (poškození dobrého jména konkurence)
- Investice obránce musí být adekvátní k překonání motivace útočníka
- Pár příkladů z reálného světa

Příklad 1: ICT infrastruktura (~250 zaměstnanců)

- Předpokládám, že firma nemá extrémně hodnotné výsledky výzkumu
- Pravděpodobnost cíleného útoku je relativně malá
- Nejpravděpodobnější:
  - Neúmyslné rozšíření útoku na jinou entitu
  - Plošné (neadresné) rozšíření malware (př. ransomware)
  - Plošné skenování Internetu na zranitelnosti
- Ideální postup:
  - Externí penetrační test (dle rozsahu 3-7MD)
  - Efektivní školení zaměstnanců

Příklad 2: Phishing

Fri 21-Feb-20 12:40 PM

ceskaposta.cz <upozorneni@cp-mailer.cz>

Nedoručení zásilky č. 5357343

To Pozděna Martin

Česká pošta

Dnes jsme se znovu neúspěšně pokusili doručit vaši zásilku, protože na uvedené adrese nebyl nikdo přítomen. V den doručení zásilky musí na uvedené adrese přítomen někdo, kdo zásilku převezme.

Druh zásilky: expresně do 1 dne.
Velikost zásilky: Velká, plochá krabice
Upozornění na doručení: zasláno e-mailem (viz digitální kopie)

Pro opětovné naplánování doručení zásilky navštivte naši nejbližší kancelář a doneste vytištěnou kopii Karty upozornění o doručení.

Elektronickou kopii Karty upozornění o doručení ve formátu Microsoft Word lze stáhnout z naší internetové stránky:
https://zakaznickyservisceskaposta.cz/go/TrackConfirmAction?action=download&invoice?5357343

Číslo sledování zásilky lze najít na Kartě upozornění na doručení a lze ho použít ke sledování vaší zásilky:
https://www.postaonline.cz/trackandtrace

Děkujeme, že využíváte naše služby

Česká pošta a.s.

Příklad 2: Phishing

- „Neškolený“ zaměstnanec **>30% míra selhání**
- „Školený“ zaměstnanec **<5% míra selhání** (do 1 roku)
- Provádíme simulované phishingové kampaně:
  - Emaily
  - USB paměti
  - Vishing
  - ReportPhishing do Outlooku
- Relativně levné a velmi účinné
- **Vhodné i jako argument pro založení rozpočtové kapitoly bezpečnost**

Příklad 3: Vy

- Každá infrastruktura / produkt unikátní
- Armádní jednotka vs automat na limonádu
- Výrobní firma vs high-tech výzkumné pracoviště
- Nenabízíme standardizovaná řešení
- Kick-off workshop k optimálnímu nastavení požadavků
- **Jsem k dispozici k hlubší diskuzi na toto téma**

O mně / O nás

- 4 roky v Auxilium Cyber Security (penetrační tester, konzultant)
- Od března 2019 mám na starost českou pobočku
- 30 zaměstnanců v Karlsruhe + 5 v Praze
- Hlavní zaměření české pobočky:
  - Penetrační testy korporátní ICT infrastruktury
  - Penetrační testy webových aplikací
  - Penetrační testy desktopových aplikací
  - Simulovaný phishing – „Penetrační testy zaměstnanců“
  - Testování IoT jednotek (automotive, armáda)
- Neváhejte se na nás obrátit pro nezávaznou konzultaci

Děkuji za pozornost

Auxilium Cyber Security

info@auxiliumcybersec.cz

+420 739 467 470