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 „zlikvidovat“ ICT firmy se 75000 zaměstnanci?**

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

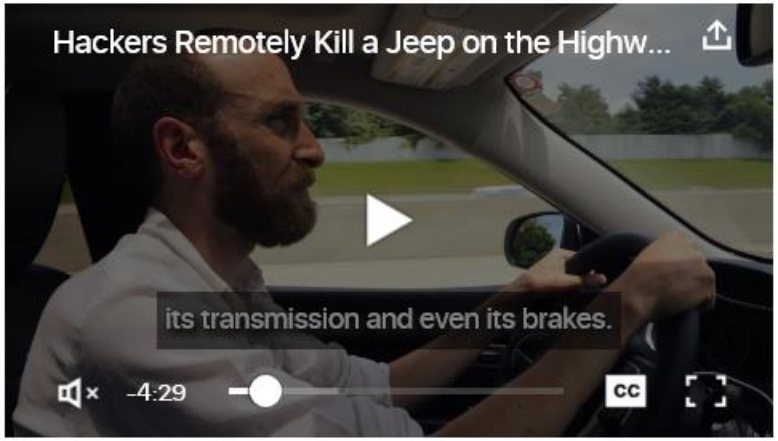
- Infrastruktura postavená na Microsoftu
- SMB zranitelnost **EternalBlue** (CVE-2017-0144)
- Patch zveřejněn v březnu 2017
- Útok NotPetya proběhl na konci června 2017
- Maersk přišel o 4000 serverů, 45000 PC a 2000 aplikací
- Infrastrukturu se podařilo obnovit za 10 dní
- Za cenu 250-300 milionů dolarů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

- Ředitel Maersk mluvící o tomto incidentu: 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)
  - Využívání endpoint protection řešení

Příklad 2: Webová služba na správu informací

- Opět záleží na potenciální motivaci a příležitosti pro útočníka:
  a. Hodnota informací
     - Zdravotní dokumentace
     - Spisová služba státní správy
     - Modelářské fórum
  b. Veřejně přístupný (Internet) vs interní (LAN)

	Zdravotní dokumentace	Spisová služba st. spr.	Modelářské fórum
Veřejný	Zavedení SSDLC	Pentest každý release	Audit (1-2 MD)
Interní	Pentest každý release	Audit (1-2 MD)	Nic

Příklad 3: IoT/automotive produkt

- Co se stane za předpokladu, že útočník převezme kontrolu:

1. Nad řízením auta/vlaku/výrobní linky
    - Zavedení SSDLC – školení vývojářů, release testy, bezpečnostní revize architektury
2. Umožní zákazníka sledovat (Alexa, webová kamera, atd)
    - Pentest každý release

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 + 4 v Praze
- Hlavní zaměření české pobočky:
  - Testování jednotek do automobilového průmyslu
  - Penetrační testy korporátní ICT infrastruktury
  - Penetrační testy webových aplikací
  - Penetrační testy desktopových aplikací
- Neváhejte se na nás obrátit pro nezávaznou konzultaci

Děkuji za pozornost

Auxilium Cyber Security

info@auxiliumcybersec.cz

+420 739 467 470