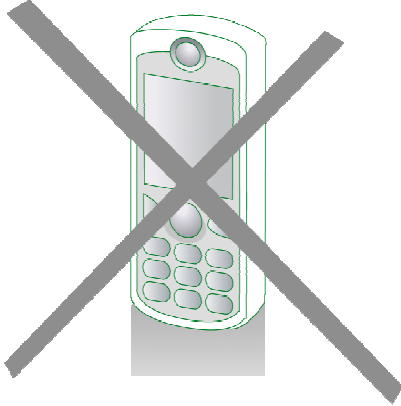




# Ethical hacking kao dio upravljanja sigurnošću

Hrvoje Šegudović, CISA, CISM, CISSP-ISSAP, CISSP-ISSMP  
<Hrvoje.Segudovic@infigo.hr>




**10 godina**  
Prvi po izboru polaznika  
1998 • 2008

**ALGEBRA**  
UČILIŠTE



**EC-Council** Accredited Training Center



## Sadržaj



10 godina  
Prvi po izboru polaznika  
1998 - 2008



- Što je *ethical hacking*
- Zakonska regulativa u RH
- Standardi i dobre prakse
- Upravljanje informacijskom sigurnošću

## Što je ethical hacking



10 godina  
Prvi po izboru polaznika  
1998 - 2008



- *Ethical hacking (white hat hacking)*
  - istraživački rad (eng. *security research*)
    - pronalaženje sigurnosnih propusta u operacijskim sustavima, komercijalnim i *open-source* aplikacijama...
    - u skladu s profesionalnom etikom
      - RFP policy (<http://www.wiretrip.net/rfp/policy.html>)
      - Symantec (<http://www.symantec.com/research/Symantec-Responsible-Disclosure.pdf>)
  - komercijalni penetracijski testovi/ispitivanja sigurnosti
    - u strogo kontroliranim uvjetima
    - u skladu s opsegom i metodologijom ispitivanja



## Zakonska regulativa u RH



10 godina  
Prvi po izboru polaznika  
1998 - 2008



### ○ Kazneni zakon (2004.)

- promjene bazirane na Konvenciji o kibernetičkom kriminalu
- čl. 223 - Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava
  - (1) Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnom sustavu...
  - (2) Tko s ciljem onemogućiti ili otežati rad ili korištenje računalnih podataka ili programa, računalnog sustava ili računalnu komunikaciju...
  - (3) ...kaznit će se tko neovlašteno oštetiti, izmijeniti, izbriše, uništi ili na drugi način učini neuporabljivim ili nedostupnim tuđe računalne podatke ili programe

## Zakonska regulativa u RH



10 godina  
Prvi po izboru polaznika  
1998 - 2008



### ○ Kazneni zakon

- članak 223. (cont)
  - (4) ...kaznit će se tko presretne ili snimi nejavni prijenos računalnih podataka koji mu nisu namijenjeni prema računalnom sustavu, iz njega ili unutar njega, uključujući i elektromagnetske emisije računalnog sustava koji prenosi te podatke, ili tko omogućiti nepozvanoj osobi da se upozna s takvim podacima
  - (6) Tko neovlašteno izrađuje, nabavlja, uvozi, raspačava, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne podatke ili programe stvorene ili prilagođene za činj enje kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka...



## Zakonska regulativa u RH



10 godina  
Prvi po izboru polaznika  
1998 - 2008



- Kazneni zakon
  - članak 223.a – Računalno krivotvorenje
  - članak 224.a – Računalna prijevarena
- Zakon o informacijskoj sigurnosti
  - državna tijela, lokalna uprava
  - sigurnosna akreditacija sustava?
    - Zavod za sigurnost informacijskih sustava
    - CERT
- Afirmativni propisi eksplicitno ne postoje!
  - npr. obveza provođenja ispitivanja sigurnosti

## Standardi i dobre prakse



10 godina  
Prvi po izboru polaznika  
1998 - 2008



- Afirmativni
- ISO 27001 / 27002 (ISO 17799)
  - 4.2.3 Monitor and review the ISMS
    - b) Undertake regular reviews of the effectiveness of the ISMS taking into account results of security audits...
  - A.15.2.2 Technical compliance
    - Information systems should be regularly checked for compliance with security implementation standards
    - ...If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable...

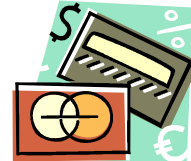
## Standardi i dobre prakse



10 godina  
Prvi po izboru polaznika  
1998 - 2008



- PCI DSS - Payment Card Industry Data Security Standard  
<https://www.pcisecuritystandards.org/>
- primjenjiv na sve sustave koji pohranjuju, procesiraju ili prenose brojeve kreditnih kartica
- Requirement 11: Regularly test security systems and processes
  - ...Run internal and external network vulnerability scans at least quarterly and after any significant change in the network...
  - ...Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification...



## Standardi i dobre prakse



10 godina  
Prvi po izboru polaznika  
1998 - 2008



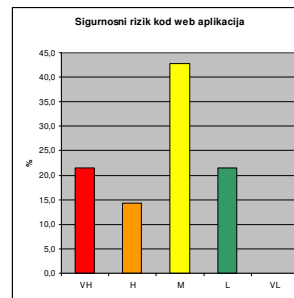
- COBIT
  - DS5 Ensure system security
    - CMM model razine 3 (defined) - 5 (optimized) zahtijevaju provođenje ispitivanja sigurnosti
- Dobra praksa
  - podrazumijeva provođenje ispitivanja sigurnosti
    - kao dio testiranja sustava/aplikacija prije puštanja u produkciju
    - redovito tijekom životnog ciklusa sustava
      - opseg i metodologija ovisi o važnosti sustava (informacija)



## Upravljanje informacijskom sigurnošću



- Zašto su ispitivanja sigurnosti uopće potrebna?
  - ispunjavanje zakonskih/regulatornih obveza
  - **razumno upravljanje inf. sustavom** –
    - revizija (kontrola) efikasnosti sigurnosnih kontrola
    - stvarna potreba za ispravljanjem sigurnosnih propusta
  - naša iskustva
    - više od 30 različitih ispitivanja sigurnosti
    - >35% Web aplikacija ozbiljno ranjivo
    - niti jedna Web aplikacija bez potrebe za bar malim unapređenjem



10 godina  
Prvi po izboru polaznika  
1998 - 2008



ALGEBRA  
UČILIŠTE



## Upravljanje informacijskom sigurnošću



- Kako odabrati cilj, opseg i metodologiju testiranja?
  - definirano regulatornim/zakonskim obvezama
  - **na temelju procjene rizika (ili važnosti sustava odnosno informacija)**
  - nekoliko mogućih pristupa:
    - provjera ranjivosti (eng. *vulnerability scan*)
    - ispitivanje sigurnosti, penetracijsko testiranje (eng. *penetration test*)
    - revizija programskog koda (eng. *code audit*)
    - revizija sigurnosti (eng. *security audit*)

10 godina  
Prvi po izboru polaznika  
1998 - 2008



ALGEBRA  
UČILIŠTE



## Upravljanje informacijskom sigurnošću



- Kako odabrati cilj, opseg i metodologiju testiranja?
  - svaki pristup ima prednosti i nedostatke
  - provjera ranjivosti (*vulnerability scan*) ≠ penetracijsko testiranje (*penetration test*)
  - provjera ranjivosti – kvartalno ili polugodišnje na kompletnoj mreži
    - ključni aspekti
      - uočavanje i eliminacija tzv. *false positives*
      - praćenje trendova
  - ispitivanje sigurnosti/penetracijsko testiranje
    - na godišnjoj razini/prije puštanja u produkciju
    - za ključne sustave
    - ključni aspekti
      - odabir pouzdanog i kompetentnog izvršitelja

10 godina  
Prvi po izboru polaznika  
1998 - 2008



## Upravljanje informacijskom sigurnošću



- *Ethical hacking*
  - zahtijeva sveobuhvatno tehničko znanje
  - nužan profesionalan pristup
  - prezentacija rezultata prilagođena *managementu*
- Penetracijski testovi / *ethical hacking*
  - u skladu s poslovnim zahtjevima i procjenom rizika
  - neizostavan dio procesa upravljanja informacijskom sigurnošću

10 godina  
Prvi po izboru polaznika  
1998 - 2008



Hvala na pažnji

Infigo IS d.o.o.  
Horvatovac 20  
10000 Zagreb

tel. +385 1 4662 700  
fax. +385 1 4662 701  
info@infigo.hr  
www.infigo.hr

