UVOD U NEMAČKO I EVROPSKO KRIVIČNO PRAVO VEZANO ZA KOMPJUTERE I INTERNET

Dr. Alexander Koch
Institut za pravo u mrežnoj privredi, informatičkim i komunikacionim tehnologijama
(Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie)

Plan predavanja

- Relevantni delikti.
- Nemačko krivično pravo vezano za kompjutere i Internet.
- Evropsko krivično pravo vezano za kompjutere i Internet.

Relevantni delikti

- Klasično hakersko delo – provala u tuđe računare:

- Pasivno špioniranje sistema (ping, skeniranje portova, itd.)
- aktivno špioniranje sistema (testiranje slabosti),
- Provala u tuđe sisteme,
- „Krađa“ podataka,
- Uništavanje podataka,
- Ilegalno korišćenje,
- Brisanje tragova.

Relevantni delikti

- (D) DoS napadi
- Virusi, crvi i trojanci, kao i Bot-mreže
- Phishing:

- postavljanje zamke
- korišćenje podataka.

- Birači (dialer):

- instalacija dialer-a,
- zahtevanje plaćanja.

Relevantni delikti

- ***Neće se*** tretirati:
  - Delikti vezani za autorska prava,
  - Pornografija,
  - Delikti mržnje,
  - Drugi delikti, koji samo koriste Internet kao novi medij.

„Epohe“ nemačkog krivičnog prava vezanog za kompjutere i Internet

- Klasično krivično pravo (19. i 20. vek),
- Mašinsko krivično pravo (posle 1935),
- Rano kompjutersko krivično pravo (1986),
- Aktuelno krivično pravo u vezi Interneta (2007).

„Klasično“ krivično pravo

- Prevara:
  - Problem: čovek mora da greši; ne važi, kada mašina „greši“.
  - Ali : kriminal vezan za birače (Dialer) mogao bi se obuhvatiti!
- Oštećenje imovine:
  - Obuhvatalo bi i „virtuelno“ uništenje: kompjuter sa izbrisanim operativnim sistemom je neupotrebljiv kompjuter.
- Zaključak: krivično pravo je bilo skrojeno na fizičke predmete i delujuće ljude.

„Mašinsko krivično pravo“(1935 / 69)

- Prevarom sticanjem koristi (1935):
  - Već rano je obuhvaćeno „ilegalno“ telefoniranje.
  - Phreaking (Cap’n Crunch).
  - Međutim, štite se samo „javne telefonske mreže“, nije obuhvaćena upotreba tuđeg (okupiranog) računara.
- Falsifikovanje tehničkih zapisa (1969):
  - Skrojeno na mehaničke zapise.
  - Traži se zapis koji se može „odvojiti“– Logfiles dakle nisu obuhvaćeni (moguće i drugačije stanovište!).

„Mašinsko krivično pravo“

- Zaključak: Krivično pravo se rano prilagodilo tehnologiji i obuhvatilo je mašinske proizvode i radnje.

„Rano kompjutersko krivično pravo“ (1986.)

- Neovlašćeni uvid u podatke, stara verzija („krađa podataka“):
  - Potrebno prevazilaženje zaštite pristupa.
    - Nije obuhvaćen “ping” ili pasivni “neovlašćeni uvid” u sigurnosne rupe.
    - Nema visokog zahteva pred zaštitu pristupa (takođe i loše lozinke).
  - Podaci se moraju “pribaviti”.
    - Svako „posmatranje“ podataka preko mreže pretpostavlja pribavljanje.
  - Obuhvaćena je „krađa podataka“ od strane hakera ili štetnih programa.
  - Nije bila kažnjiva prosta „provala“ u sistem (ali već prvi pogled...).

„Rano kompjutersko krivično pravo“

- Krivotvorenje podataka koji su bitni kao dokazi:
  - Krivotvorenje „hipotetičkih“ elektronskih dokumenata. Štite se samo ljudske izjave misli – npr. elektronski memorisani ugovori, ali i e-mailovi.
  - Do sada nije imalo naročitog praktičnog značaja.
  - Ali: Spam i Phishing sa falsifikovanim oznakama pošiljaoca mogu se obuhvatiti time.

„Rano kompjutersko krivično pravo“

- Izmena podataka („virtuelno“ oštećenje stvari):
  - Kopija „pravog“ oštećenja stvari.
  - Obuhvaćen je „vandalizam“ na hakerisanim sistemima;
  - Ali i izmene / manipulacija kroz viruse, crve i trojance.

„Rano kompjutersko krivično pravo “

- Izmena podataka (nastavak):
  - Dialer (birači) („klasična“ prevara slanjem računa).
    - Ali: u praksi je to prevashodno problem iz građanskog prava.
      - Sudska praksa je pomogla u praksi i odbila je zahteve za naplatu.
      - Telekomunikaciono zakonodavstvo: obaveza registracije “Dialer”-a, specijalne numeričke oznake.
      - 2005: 21.559 pritužbi kod Savezne agencije za mreže.
      - 2007 (1. polugodište): 26 pritužbi kod Savezne agencije za mreže.
  - Problem je rešen na građansko i upravno pravni način, ali ne i prema krivičnom pravu!

„Rano kompjutersko krivično pravo“

- Kompjuterska sabotaža, stara verzija:
  - „Naročito teška“ izmena podataka; obuhvaćeni su samo računari „pravnih lica“ i „preduzeća “ – ne i privatni sistemi.
  - (D)DoS-napadi.
- Kompjuterska prevara:
  - Takođe se i kompjuteri mogu obmanom dovesti u “zabludu”.
  - Upotreba podataka o računu prilikom Phishing-a.
    - Za finansijskog agenta i pranje novca.

„Rano kompjutersko krivično pravo“

- Zaključak:
  - Zakonodavstvo je reagovalo na kompjuterski kriminal iz 80-tih godina.
  - Trebalo je krivično goniti samo „zlog“ hakera, ali ne i učenika koji iz tehničke radoznalosti hakeriše tuđi sistem.
  - Kompjutersko krivično pravo iz 1986. godine bilo je u stanju da obuhvati potpuno nove pojavne oblike kompjuterskog kriminala, kao što su Phishing i (D)DoS-napadi.
  - Dakle, nije potreban poseban opis delikta prilikom pojavljivanja svake novonastale tehnike.

„Novo Internet krivično pravo“ (2007.)

- Neovlašćeni uvid u tuđe podatke, nova verzija („virtuelni upad u privatnu sferu“):
  - Nije više potrebno da se podaci “pribave”.
- Presretanje podataka:
  - Sniffing, TEMPEST (diskretno zračenje).
- Kompjuterska sabotaža, nova verzija
  - Obuhvaćeni su i privatni sistemi “od bitnog značaja”.

„Novo Internet krivično pravo“

- Priprema neovlašćenog uvida i presretanja podataka („hakerski paragraf“):
  - Programiranje i širenje „hakerskih alata“.
  - Namera zakonodavstva: potrebno je sprečiti širenje virusa, crvi i trojanaca, kao i softvera za napade.
  - Problem: Dual-use-Software: Skener slabih tačaka može se upotrebiti za provalu u tuđi sistem, ali i za proveru sopstvenog sistema.
  - Granice su potpuno otvorene.

„Novo Internet krivično pravo“

- Zaključak:
  - Više ne postoji “sportsko” hakerisanje.
  - Praktično je kažnjivo svako ponašanje koje prevazilazi prosto “posmatranje” tuđih sistema “spolja”.
  - Moguća je čak i preterana kriminalizacija; u svakom slučaju, “dobra” scena je vrlo unespokojena.

Evropsko kompjutersko i Internet krivično pravo

- Konvencija Evropskog Saveta o kompjuterskom kriminalu (Cybercrime Convention).
- Okvirni zaključak o napadima na informacione sisteme EU.

Cybercrime Convention

- Potpisala i Srbija (i Crna Gora) 7.4.2005. god. Ali još nije stupila na snagu.
- Nemačka je takođe potpisala, ali još nije stupila na snagu, iako se u velikim delovima već primenjuje.

Cybercrime Convention

- Katalog delikata koji moraju biti kažnjivi:
  - Protivpravni pristup,
  - Protivpravno presretanje,
  - Zahvat nad podacima („oštećenje stvari“),
  - Upad u sistem („ometanje rada“),
  - Zloupotreba uređaja („hakerski alati“),
  - Kompjuterski falsifikati / prevara,
  - Dečija pornografija,
  - Kršenje autorskog prava.

Cybercrime Convention

- Oblici odgovornosti:
  - Počinilac, pomagač ili podstrekač,
  - Pokušaj,
  - Pravna lica („krivično pravo za preduzeća“).
- Dodatni propisi:
  - Regulisanje minimalnih mogućnosti u istražnoj tehnici (prisluškivanje, konfiskacija),
  - Međunarodna saradnja.

Okvirni zaključak o napadima na informacione sisteme

- ***VAŽNO:*** EU, ne EZ! Ovde se ne radi o supranacionalnom pravu, nego o “prostom” međunarodnom pravu.
- „Sajber terorizam“.
- Katalog delikata koji moraju biti kažnjivi :
  - Protivpravni pristup informacionim sistemima,
  - Protivpravni upad u sistem,
  - Protivpravni zahvat nad podacima.

ZAHVALJUJEM NA PAŽNJI!

<u>Za dodatne informacije možete se obratiti:</u>

IRNIK
Dr. Alexander Koch
Postfach 15 01 61
53040 Bonn
DEUTSCHLAND
Tel.: +49-2 28-8 50 86 63
Fax: +49-2 28-8 50 86 62
ak@irnik.de
http://www.irnik.de

IRNIK

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie