

Kiberkriminal

Matej Kovačič

Fakulteta za družbene vede, Univerza v Ljubljani

Seminar preiskovalnih sodnikov v Termah Olimia v
Podčetrtku, petek, 16. 5. 2008

(CC) 2006, 2007, 2008

Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <<http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Čufarjeva ulica 17, 1000 Ljubljana.

Kiberkriminalci

Kiberkriminal

- Nekateri kiberkriminal definirajo kot vsako obliko kriminala, pri kateri je uporabljena računalniška oziroma v širšem smislu celo informacijska tehnologija.
- Vendar pa sta Douglas Thomas in Brian D. Loader mnenja, da kiberkriminal ni zgolj samo uporaba informacijsko-komunikacijske tehnologije v kriminalne namene, pač pa je bistveni element kiberkriminala v tem, da ta kriminal ne bi bil mogoč brez uporabe tehnologije, vsaj ne v takem obsegu.
 - Primer vdora v T-Mobile, kjer je napadalec prodobil dostop do podatkov o 16,3 mio. strankah.

Kiberkriminal

- Poleg tega se kiberkriminal po Reitingerju od navadnega kriminala razlikuje še po treh pomembnih značilnostih:
 - lahko je izveden na daljavo;
 - identiteto osebe, ki kaznivo dejanje izvede je mogoče razmeroma enostavno zakriti ali ponarediti;
 - poleg tega pa sledenje izvornemu komunikacijskemu sredstvu, preko katerega se je nekdo povezal v kiberprostor, ni vedno mogoče, saj napadalci pogosto uporabljajo tehniko povezovanja preko različnih sistemov (tim. *looping* ali *weaving*), kar onemogoči ali vsaj oteži sledenje).

“Hekanje”

- Izraz hekanje se večinoma uporablja za *“kompleksno mešanico legalnih in nelegalnih aktivnosti, od legitimnega kreativnega programiranja, do prepovedanega vdiranja in manipulacije svetovnih telefonskih ali računalniških sistemov”* (Taylor); najbolj pogosto pa se ga dojema kot sofisticirano ilegalno dejavnost.

“Kiberkriminalci” - prva delitev

- Thomas in Loader kiberkriminalce delita v tri kategorije:
 - hekerje in phreakerje (ang. *phreaker*; gre za “telefonske hekerje”, ki se ukvarjajo z zlorabo telefonskih sistemov; phreakerji so bili predhodniki hekerjev, formirani pa so se začeli v ZDA konec 70-tih let, v današnjem času jih skorajda ni več), ki vdirajo v sisteme večinoma iz radovednosti in ne povzročajo škode;

“Kiberkriminalci” - prva delitev

- trgovce z informacijami, katerih glavni motiv je profit;
- ter teroriste, ekstremiste in deviantneže, ki informacijske sisteme uporabljajo za nezakonite politične ali družbene dejavnosti (npr. razširjanje sovražnega govora, otroške pornografije, napade na strežnike sovražnih držav itd.).

“Kiberkriminalci” - druga delitev

- Levy pravi, da obstajajo štiri generacije hekerjev, s katerimi se je pojem hekerja spreminjal skozi čas.
 - Prva generacija, ki izvira iz MIT, je v 50-tih in 60-tih letih prejšnjega stoletja razvila prve programske tehnike.
 - Drugo generacijo predstavljajo tisti posamezniki, ki so razvili prve osebne računalnike in s tem omogočili dostop računalniške tehnologije širšim množicam.

“Kiberkriminalci” - druga delitev

- Tretjo generacijo označujejo vodilni razvijalci računalniških iger.
- Četrto pa osebe, ki na nedovoljene načine vstopajo v tuje računalnike.
- Iz te delitve tudi izhaja, da so bili prvotni hekerji predvsem ustvarjalni, zadnja generacija hekerjev pa naj bi bila že v večji ali manjši meri destruktivna.

“Heker”

- Izraz “heker” (ang. *hacker*) je prvi uporabil Joseph Weizenbaum leta 1976.
- Popularno izraz danes opisuje posameznika, ki ima veliko računalniško-tehničnega znanja, to znanje pa izkorišča za napad na računalniške sisteme, kar hekerje uvršča v polje računalniške kriminalitete.

“Heker”

- Po samodefiniciji se hekerji v hekerskem slovarju (*Jargonfile*) opisujejo kot “osebe, ki uživajo v raziskovanju računalniških sistemov in iskanju novih načinov njihove uporabe; osebe, ki navdušeno (celo obsedeno) programirajo ... osebe, ki uživajo v intelektualnih izzivih v aktivnem premagovanju in zaobhajanju omejitev”.

“Heker”

- Eden izmed slovenskih hekerjev, je v pogovoru povedal: *“ne razumem zakaj ljudje izraz hekanje vedno povezujejo z vdiranjem in asocialnimi tipi. ta termin ne pomeni nič drugega kot da si zelo dober v neki stvari, pa naj si bo to računalništvo ali kaj drugega. sem menja da je to bolj način razmisljanja, želja po znanju, izziv...”*.

“Heker”

- Bruce Schneier hekanje razume kot stanje duha, pri čemer način razmišljanja povsem ločuje od namena uporabe le-tega: *“Heker je nekdo, ki razmišlja izven okvirov. Je nekdo, ki opusti običajno modrost in namesto tega naredi nekaj drugega. Je nekdo, ki gleda na rob in se sprašuje kaj je na oni strani. Je nekdo, ki vidi niz pravil in se sprašuje, kaj se zgodi, če jim ne slediš. Heker je nekdo, ki eksperimentira z omejitvami sistema zaradi intelektualne radovednosti. ...”*

“Heker”

- *“Računalniki so odlično igrišče za hekerje. Računalniki in računalniška omrežja so ogromni zakladi skrivnega znanja. Internet je brezmejna pokrajina neodkritih informacij. Več kot veš, več lahko storiš. ... To je varnostno hekanje: vdiranje v sisteme s pomočjo razmišljanja na drug način. ‘Heker’ je stanje duha in nabor veščin; kako to uporabiš, pa je drugo vprašanje.” (Schneier).*

“White hat” vs. “Black hat”

- S samodefinicijo hekerjev se vzpostavlja tudi delitev na tim. “črne” (ang. *black hat*) in “bele” (ang. *white hat*) hekerje.
- Tim. “beli hekerji” poudarjajo, da spoštujejo določena etična načela, predvsem se izogibajo namernemu povzročanju škode.
- “Črni hekerji”, včasih jih označujejo tudi z izrazom kreker (ang. *cracker*), pa so osebe, ki hekersko znanje zlorablja za slabe namene, predvsem nezakonito vdiranje v računalnike s pridobitnimi nameni ter povzročanje škode.

“Cracker”

- Izraz kreker (ang. *cracker*) se sicer uporablja tudi za posameznike, ki se ukvarjajo s tim. reverznim inženiringom programske opreme, predvsem z namenom razbijanja zaščite programov prek kopiranjem.

“Script kiddie”

- Skriptarji (ang. *script kiddies*) so osebe, ki nimajo pretiranega računalniškega znanja, pač pa za vdore uporabljajo javno dostopna vdiralska orodja, ki so jih razvili drugi.
- Če so krekerji praviloma visoko motivirani in vdirajo v točno določene sisteme, pa skriptarji navadno ne iščejo točno določenih žrtev, pač pa po internetu povsem naključno iščejo slabo zaščitene računalnike, v katere potem poskušajo vdreti.
- Motivi so večinoma samodokazovanje, zabava ali vandalizem.

“Script kiddie” vs. “heker”

- Eden izmed slovenskih hekerjev je skriptarje opisal takole: *“srečujem jih skoraj vsakodnevno na raznih forumih. Mulci, ki mislijo, da bodo oboroženi z Sub7 (gre za znano hekersko orodje oz. trojanskega konja, m. op.) in XP-ji osvojili svet. Nimajo želje po znanju in si želijo vse instantno. Njihov edini motiv je bahanje”*.
- Izjava 16-letnega britanskega študenta Richarda Prycea, znanega tudi kot Datastream Cowboy, ki je leta 1994 vdrl v več visoko zaupnih ameriških vojaških sistemov: *“Nekateri so gledali televizijo po šest ur na dan, jaz pa sem hekal računalnike.”*.

“Haktivizem”

- Obstajata dve definiciji “haktivizma”:
 - nudenje informacijske (tehnične) podpore političnim aktivistom (praviloma povsem zakonito);
 - nelegalno politično delovanje na spletu. Denningova ga definira kot povezavo med aktivizmom (pri katerem gre za uporabo interneta v namene širjenja informacij, debatiranje, načrtovanje in koordinacijo političnih in družbeno angažiranih aktivnosti, itd., skratka legitimno uporabo, ki ni dekstruktivna) in hekanjem.

“Haktivizem”

- Po njeni definiciji je haktivizem sicer v osnovi dejavnost **povzročanja motenj**, ne pa tudi resni škodi.
- Kot primere navaja:
 - virtualno zasedništvo (razobličjenja spletnih strani),
 - virtualne blokade (politično ali aktivistično motivirani DOS napadi),
 - pošiljanje poštnih bomb,
 - vdore ter širjenje računalniških virusov in črvov (Denning).

Informacijsko obveščevalni napadi

- Severna Koreja (Mirrim College)
- Kitajska (sile kibernetске varnosti, katerih naloga je tudi izvajanje kibernetских napadov in vzpostavitev vohunskih mrež za delovanje v informacijsko komunikacijskih omrežjih)
 - Titan Rain (2003 - 2005);
 - svarilo direktorja MI5 leta 2007;
 - kitajska civilna kiber milica (napadi na aktiviste za podporo Tibetu).

“Kiberterorizem”

- Za uporabo hekerskih tehnik v aktivistične a destruktivne namene (npr. povzročanje ekonomske škode ali ogrožanje življenja ljudi) Denningova uporablja izraz kiberterorizem.
- Nekateri so mnenja, da kiberterorizem kot ena izmed zvrsti terorizma sploh ne obstaja oz. gre za bolj teroretični pojem (npr. Schneier v *Beyond Fear*).

“Kiberterorizem”

- Kljub temu sta na internetu znana vsaj dva primera varnostnih incidentov, ki bi ju glede na definicijo Dorothy E. Dennig lahko šteli za kiberterorizem:
 - *911 worm*, računalniški virus, ki se je pojavil aprila 2000 in je po uspešni okužbi skušal z modemom klicati na številko za klic v sili (v ZDA je to številka 911);
 - julija 2002, je nekdo napisal virus, ki je zamenjal klicne številke uporabnikov storitve WebTV s številko 911;
 - napad na pristaniške v Houstonu leta 2003;
 - pogojno: napad SQL Slammerja na jedrsko elektrarno v Ohio leta 2003.

Škodljiva in koristna uporaba znanja

- *“Najbolj mi je bil pa zanimiv en ddosnet [prikrito omrežje namenjeno DDOS napadom, m. op.] od enega 17-let starega fanta z okolice Novega mesta. Ta je imel stvari narejene tako, da je za okužbo uporabil RX-e, potem jih je pa nadomestil z svojim programom napisanim v delphiju. ddosnet je bil majhen, kake 70 računalnikov. Šel sem tako daleč, da sem prišel do imena in priimka. Poklical, dobil na telefon mamó in izvedel še ostale podatke. Fanta sem zanimiral za povsem druge stvari. Danes piše komercialne programe. Z enim res dobrim programom v delphiju, je zaslužil malo manj kot 1000 EUR.”*

Klasifikacija napadov

Nekatera kiberkriminalna dejanja

- Pošiljanje nezaželene elektronske pošte
- Razobličanja spletnih strani
 - XSS napadi
- Internetne goljufije in prevare
- Zlonamerno (vohunsko) programje
- Prikrita omrežja in napadi s poplavljanjem
- Vdor v informacijski sistem
- Prestrezanje
 - Napad s posrednikom
 - Prestrezanje v brezžičnih omrežjih in kraja dostopa do interneta
 - Tajnost e-pošte, prestrezanje komunikacij zaposlenih in zasebnost na delovnem mestu

Pošiljanje nezaželene elektronske pošte

- Ni kaznivo dejanje, pač pa prekršek, ki ga obravnavajo naslednji zakoni:
 - *Zakon o varstvu potrošnikov,*
 - *Zakon o elektronskih komunikacijah,*
 - *Zakon o varstvu osebnih podatkov,*
 - *Zakon o elektronskem poslovanju na trgu.*
- Lahko vodi do kaznivega dejanja:
 - pošiljanje virusov,
 - poskusi prodaje lažnih ali goljufivih izdelkov (npr. ponarejenih zdravil),
 - poskusi prevare z namenom zbiranja osebnih podatkov ali dostopnih gesel.

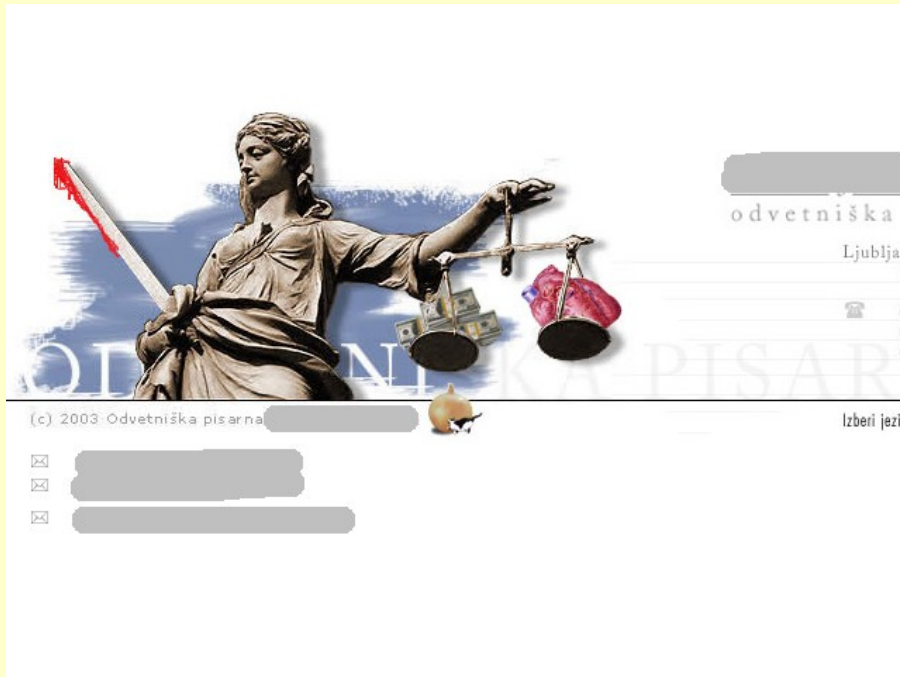
Razobličjenja spletnih strani

- Razobličjenje (ang. *defacement*): napadalec spremeni vsebino spletne strani.
 - novodobne oblike vandalizma oz. pisanja grafitov,
 - politični motivi,
 - maščevanje ali škodovanje "konkurenci",
 - poskusi goljufije!
- Motivi: samodokazovanje in dolgočasje, iskanje medijske pozornosti in tekmovanje med razobličevalskimi skupinami, pridobitni motivi.
- Praviloma je razobličjenje posledica vdora **in** spremembe informacijskega sistema.

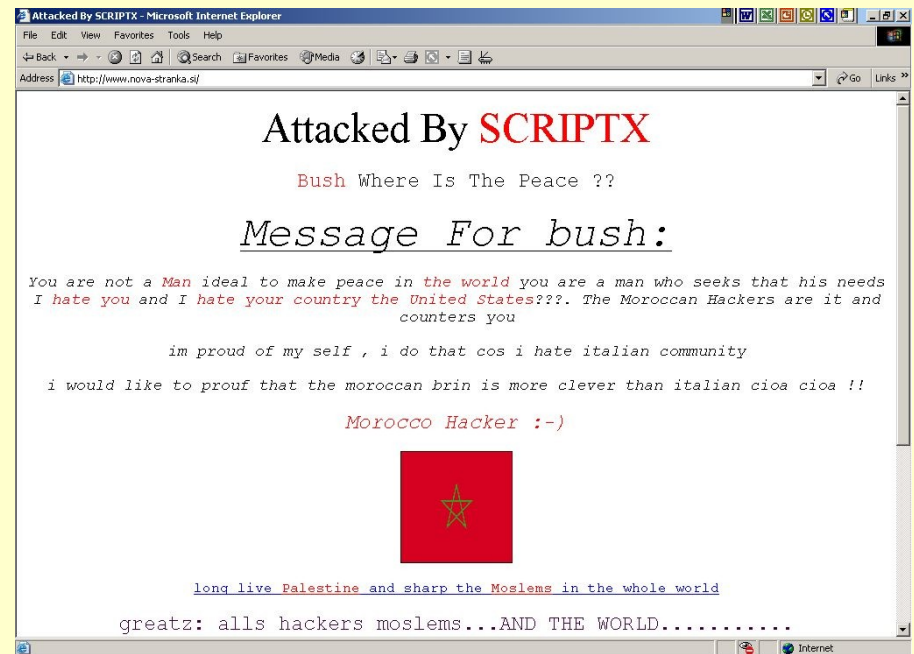
Razobličjenja spletnih strani (z XSS napadom)

- XSS napad (*Cross-site Scripting*): navzkrižno izvajanje skriptov na spletnih straneh.
- Gre za tehniko, ki se izvaja v uporabnikovem spletnem brskalniku in ne na strežniku.
- Ni vdora v informacijski sistem, le sprememba prikaza spletne strani **pri uporabniku**.

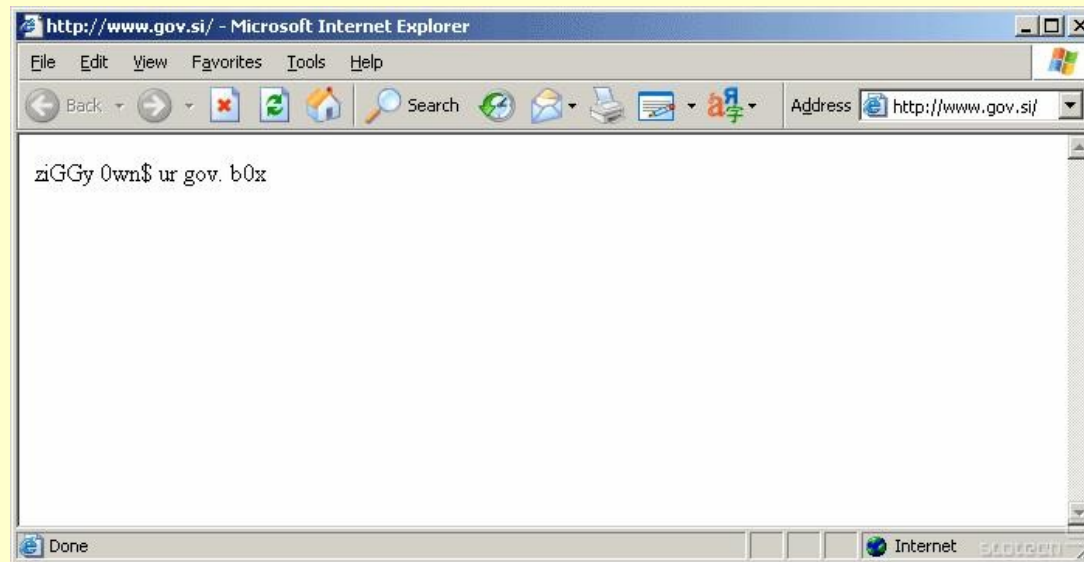
Primeri...



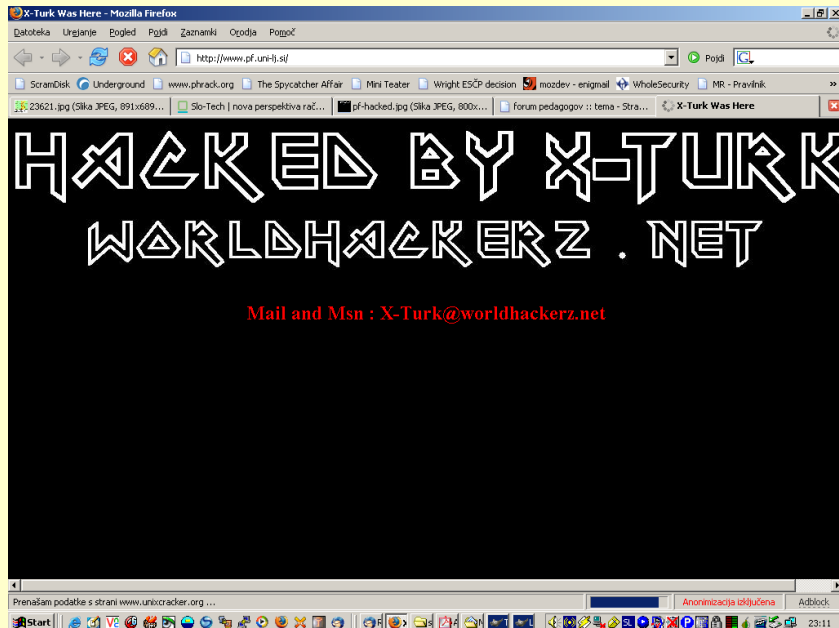
Razobličena spletna stran odvetniške pisarne.



Razobličenje spletne strani politične stranke.



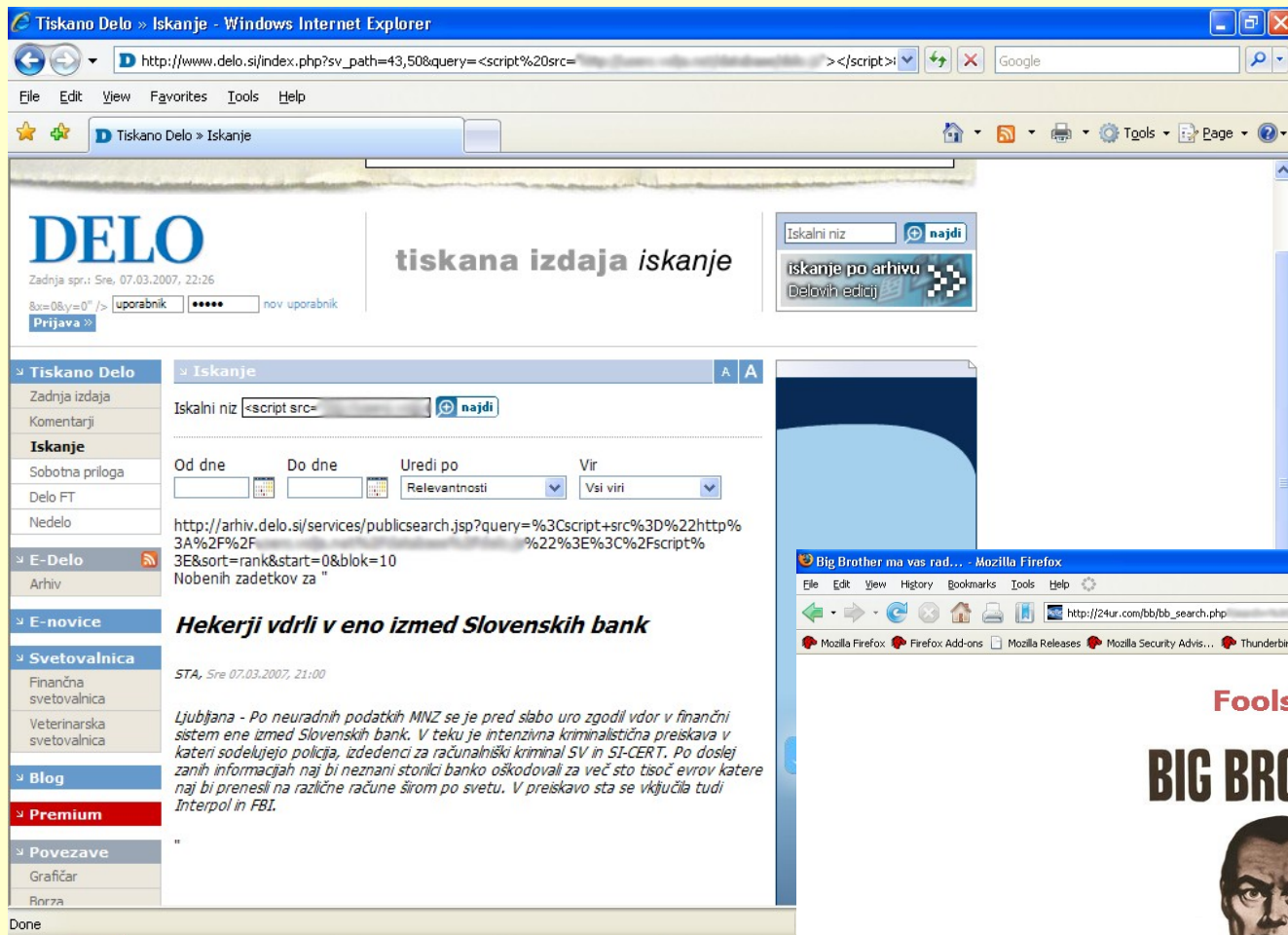
Razobličenje vladne strani (gov.si).



Pravna fakulteta, Univerza v Ljubljani (razobličenje).



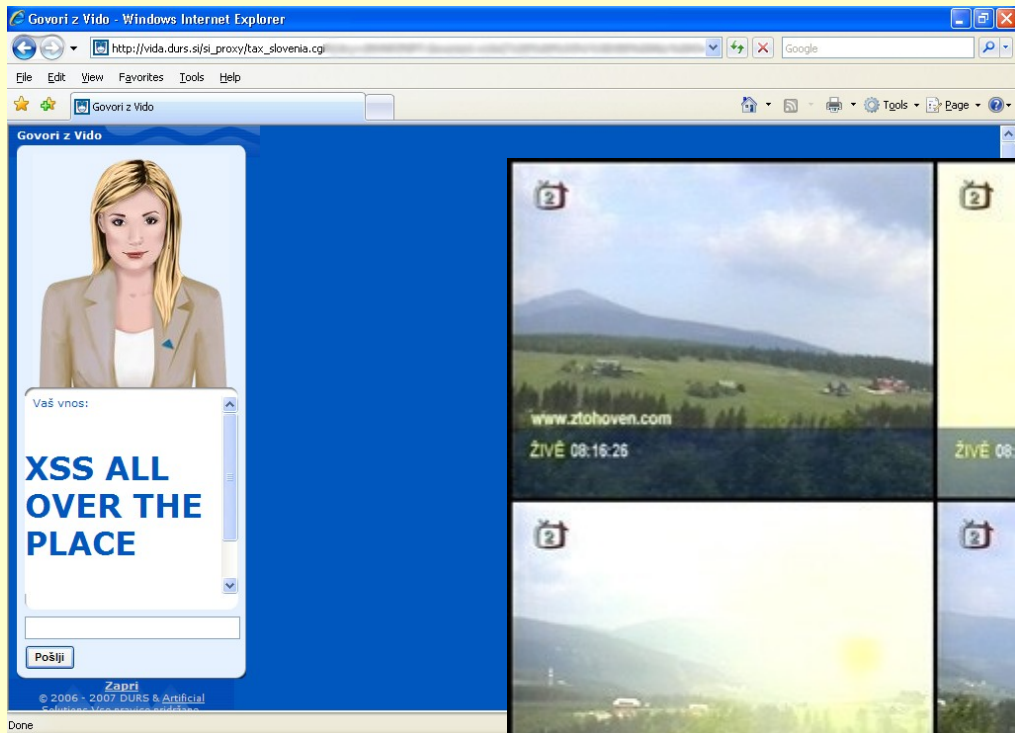
Razobličenje spletne strani rimokatoliške cerkve.



Lažna novica na spletni strani časnika DELO (XSS napad).



"Big Brother" na 24ur.com (XSS napad).



XSS napad na
"davčno Vido".

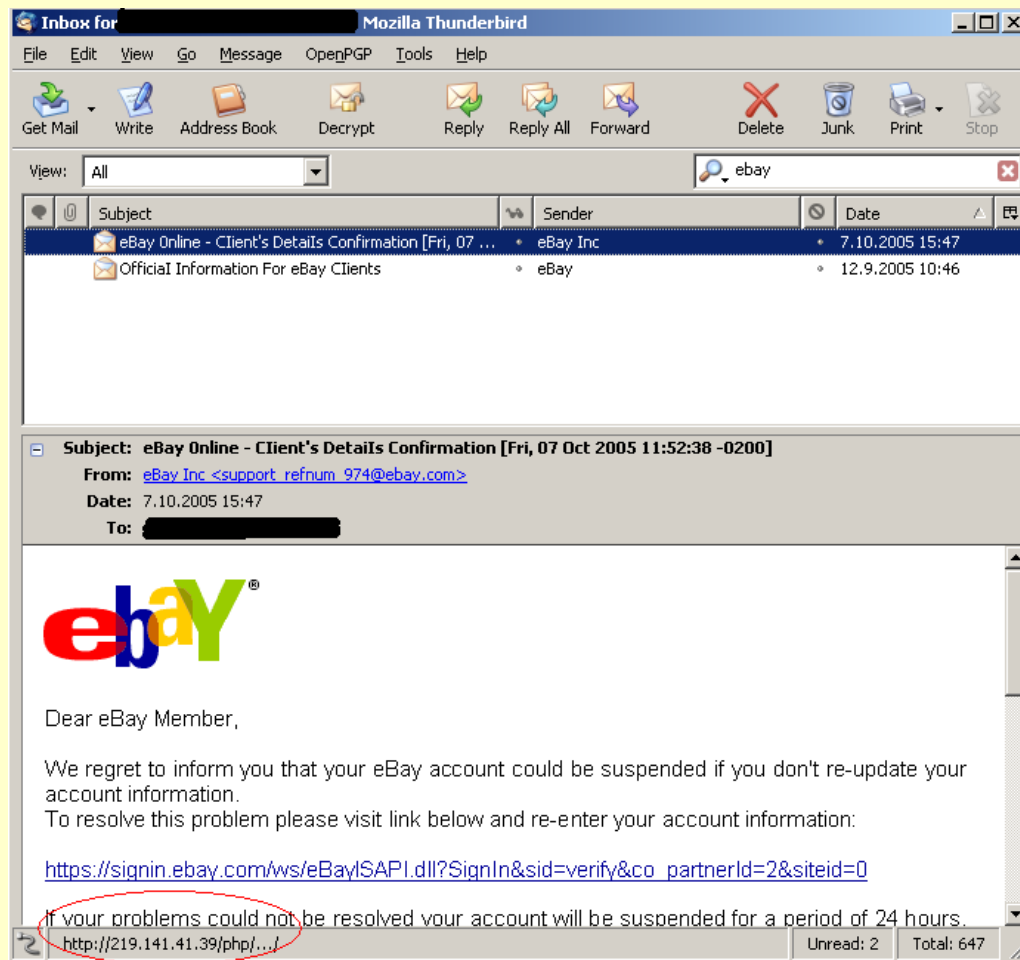


Lažna jedrska eksplozija vrinjena v živi video prenos
na eni izmed čeških TV postaj leta 2006.

[prikaz videoposnetka]

Internetne goljufije in prevare

- Socialni inženiring (ang. *social engineering*);
- ribarjenje (ang. *phishing*);
- pharming napad (napadalec pomočjo DNS preusmeritev uporabnike usmerja na lažne spletne strani);
- scam 419 (nigerijska prevara).



Primer ribarjenja (phisinga) preko neželene e-pošte.

Zlonamerno (vohunsko) programje

- “*Spyware*” (programska oprema namenjena zbiranju podatkov o uporabniku), “*adware*” (programska oprema namenjena prikazovanju oglasov), “*malware*” (zlonamerna programska oprema namenjena izključno nezakonitim dejavnostim).
 - Primer: klicalniki (ang. *dialer*), zamenjajo telefonsko številko ponudnika dostopa do interneta v uporabnikovih nastavitvah omrežja na klic;
 - korenski kompleti (ang. *rootkit*), so namenjeni prevzemu popolnega nadzora nad računalnikom in skrivanju napadalca v sistemu.

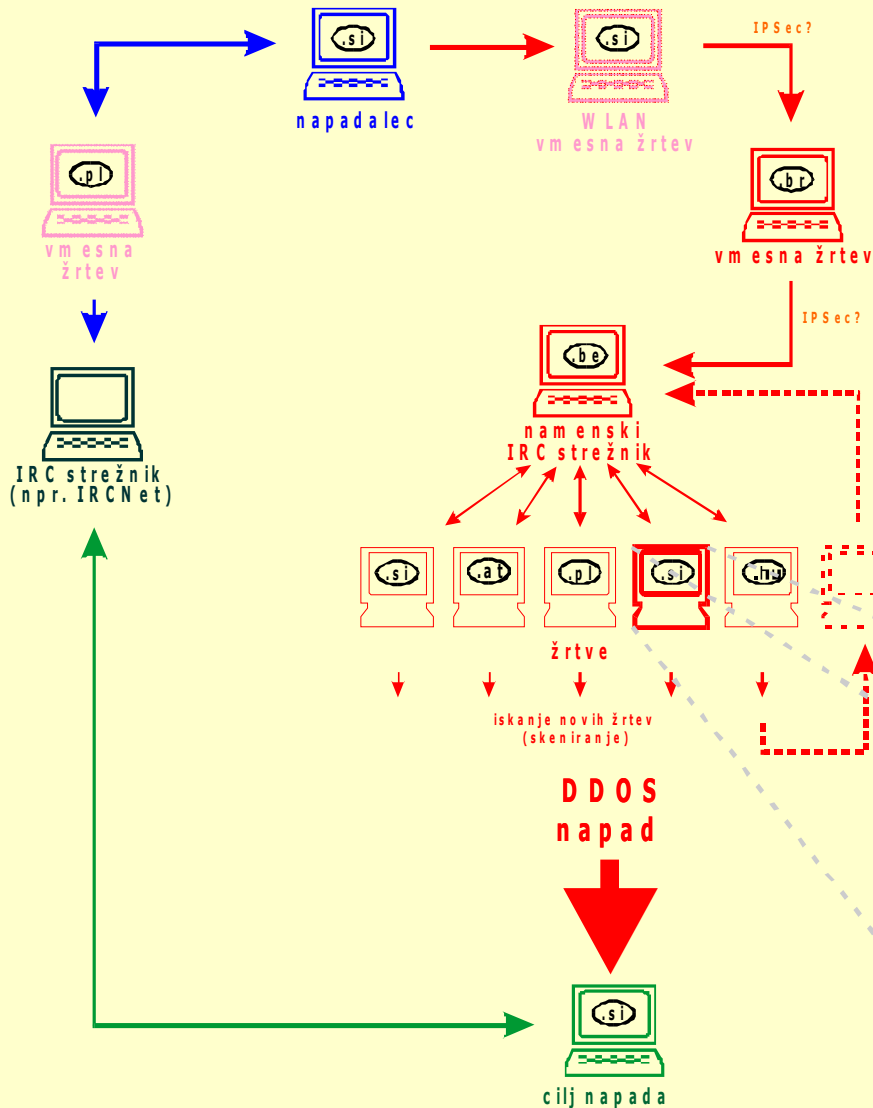
Prikrita omrežja in napadi s poplavljanjem

- Napadi s poplavljanjem so napadi na razpoložljivost sistema oziroma oviranje njegovega delovanja:
 - DOS (ang. *Denial Of Service*) napadi
 - DDOS (ang. *Distributed Denial Of Service*) napadi
- Prikrito omrežje (*botnet* - izraz izvira iz besed '**robot**' ter '**network**').
- Ka začetku se uporabljajo večinoma zgolj za izvajanje napadov s poplavljanjem v času tim. IRC vojn.
- Kasneje čedalje bolj prihaja do zlorabe v kiberkriminalne namene:
 - skrivanje spletnih strežnikov (*invisible bulletproof hosting*),

Prikrita omrežja in napadi s poplavljanjem

- pošiljanje nezaželene elektronske pošte,
- kraja osebnih podatkov in podatkov za elektronsko bančništvo, itd.
- JavaScript ugrabljanje oz. spletni virusi (Jitko).
- Prikrita omrežja nove generacije (*Storm, Gozi, Nugache,...*):
 - za komuniciranje uporabljajo P2P princip (ni enega Command&Control centra);
 - točke v omrežju med seboj komunicirajo po šifriranih kanalih;
 - programska koda uporablja različne načine prikrivanja (mutatorji programske kode, stiskanje in šifriranje kode);
 - *Nugache*: prva povezava v internet šele po mesecu dni.

Shema prikritega omrežja:

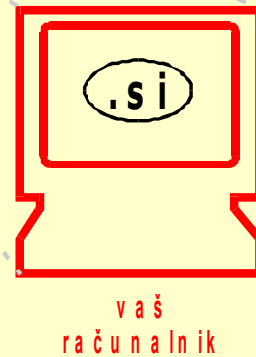


```

mlIRC - [#dml [566] [+mnst]: was IT The RED Wire or was it The Blue one]
File Tools DCC Commands Window Help
* code[2000504] has left #dml
<code[200010763]> found: 64.85.14.129 attempting to infect...
* code[200060406] has left #dml
* code[20004900] has left #dml
* code[200018090] has joined #dml
* code[200015395] has joined #dml
<code[200010763]> found: 161.184.8.143 attempting to infect...
* code[200093350] has left #dml
* code[200048300] has left #dml
<code[200010763]> found: 65.220.48.103 attempting to infect...
<code[200010763]> found: 211.52.231.185 attempting to infect...
* code[200028696] has joined #dml
* code[200043316] has joined #dml
* code[200080050] has joined #dml
* code[200020713] has left #dml
<code[200010763]> found: 162.15.190.130 attempting to infect...
<code[200010763]> found: 159.69.221.24 attempting to infect...
<code[200010763]> found: 156.34.68.108 attempting to infect...
* code[200063294] has left #dml
<code[200010763]> found: 198.174.40.72 attempting to infect...
<code[200010763]> found: 208.37.47.29 attempting to infect...
* code[200061099] has joined #dml
* code[200031867] has left #dml
<code[200010763]> found: 158.123.28.211 attempting to infect...
* code[200080028] has left #dml
* code[200043984] has left #dml
* code[200089080] has joined #dml
<code[200010763]> found: 198.59.69.203 attempting to infect...

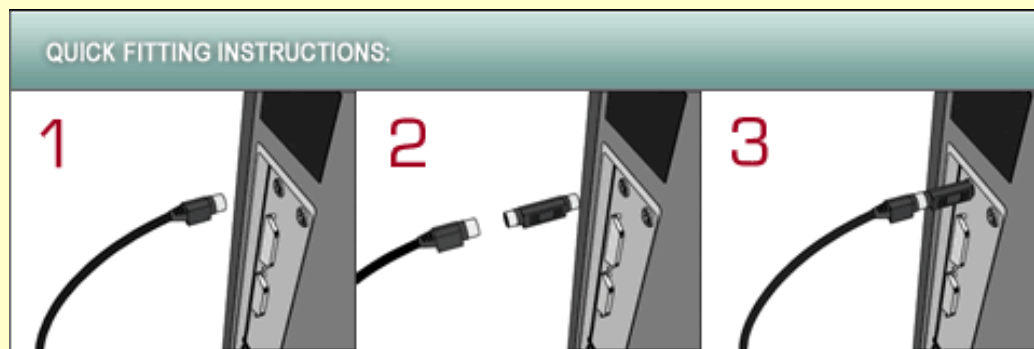
```

Pogled na prikrito omrežje s strani napadalca.



Vdor v informacijski sistem

- Fizični dostop (kraja, izguba, nepooblaščen dostop do prostorov, kjer se nahaja računalniška oprema, podtikanje strojnih in programskih dodatkov).
- Problem razmejitve med javnim in zasebnim prostorom na internetu.
 - Google hacking (iskanje javno dostopnih informacij)
- Motivi za klasičen vdor:
 - kraja podatkov in sistemskih sredstev,
 - podtikanje podatkov in izsiljevanje ali maščevanje,
 - prikrivanje ("odskočna deska" za kasnejše napada),
 - radovednost, priložnost,...
- Vdiralska orodja in tehnike razmeroma lahko dostopne
 - Primer: za izvedbo SQLI zadostuje že spletni brskalnik
- Ogroženi niso samo računalniki! [**prikaz vdora v bankomat**]



Strojni prestrezniki tipkanja (vir in avtorstvo: www.keyghost.com)

Prestrezanje komunikacij

- Prestrezanje (*packet sniffing*, na internetu tehnično lažje izvedljivo kot v telefonskih omrežjih)
 - prestrezanje internetne telefonije (VoIP): primer MediaDefender leta 2007
- Izvedba mogoča tudi z legitimnimi orodji za analizo omrežij.
- Napad s posrednikom (MITM napad), za napad na (SSL) šifrirane komunikacije. [[prikaz napada na Gmail](#)]
- Prestrezanje v brezžičnih omrežjih in kraja dostopa do interneta (odprta omrežja, kriptanaliza WEP, WPA, *wardriving*). [[prikaz kriptanalize WEP](#)]
 - Primer vdora v poštno banko v Haifi.

Zasebnost na delovnem mestu

- Tajnost e-pošte, prestrezanje komunikacij zaposlenih in zasebnost na delovnem mestu:
 - **Halford proti Veliki Britaniji** iz leta 1997: ESČP je v razsodbi izrecno zapisalo, da zaposleni na delovnem mestu upravičeno pričakuje zasebnost.
 - **Copland proti Veliki Britaniji** iz leta 2007: ESČP je v zvezi z uporabo interneta in elektronske pošte na delovnem mestu delavki priznalo širok krog pravice do zasebnosti in presodilo, da je delodajalec neupravičeno posegal v njeno zasebnost. Ključni element sodbe je, da delavka ni bila vnaprej opozorjena, kdaj in v kakšnih primerih lahko delodajalec nadzira e-pošto.

Zasebnost na delovnem mestu

- Odločitev Kasacijskega sodišča Francije v primeru **Societe Nikon France, SA v. Onof**, št. 99–42.942 iz leta 2001:
»delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema preko službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah ... To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene... Podjetje ali druge ustanove ne smejo biti mesta, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave ... Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti.«

Kazensko pravni vidiki

Kazenski zakonik RS

- V *Kazenskem zakoniku* (KZ) so kot kazniva dejanja, ki bi jih lahko šteli med tim. računalniška kazniva dejanja oziroma kazniva dejanja, ki jih je mogoče izvesti s pomočjo računalniška oz. informacijske tehnologije, opredeljena naslednja ravnanja:
 - neupravičeno prisluškovanje in zvočno snemanje (148. člen KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
 - neupravičeno slikovno snemanje (149. člen KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");

Kazenski zakonik RS

- kršitev tajnosti občil (2. točka 2. odstavka 150. člena KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- nedovoljena objava zasebnih pisanj (151. člen KZ, v osnovi ne gre za tim. "računalniško kaznivo dejanje");
- zloraba osebnih podatkov (2. odstavek 154. člena KZ);
- kršitev avtorske pravice (2. odstavek 158. člena KZ);
- neupravičeno izkoriščanje avtorskega dela (159. člen KZ);

Kazenski zakonik RS

- kršitev avtorski sorodnih pravic (160. člen KZ, v osnovi ne gre za tim. “računalniško kaznivo dejanje”);
- neupravičen vstop v informacijski sistem (225. člen KZ);
- vdor v informacijski sistem (242. člen KZ);
- izdelovanje in pridobivanje orožja in pripomočkov namenjenih za kaznivo dejanje - pripomočke za vdor ali neupravičen vstop v informacijski sistem (3. odstavek 309. člena KZ).

Kršitev tajnosti občil

150. člen KZ (predlog novega KZ-1: 139 člen)

...

(2) Z denarno kaznijo ali z zaporom do enega leta se kaznuje:

2) kdor se z uporabo **tehničnih sredstev** neupravičeno seznaní s sporočilom, ki se prenaša po telefonu ali s kakšnim drugim **telekomunikacijskim sredstvom**;

...

(5) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, poštni **ali drug delavec**, ki mu je zaupano prevzemanje, prenos ali predaja tujih pisem, tujih brzojavk ali kakšnih drugih pisanj ali pošiljk, se kaznuje z zaporom od treh mesecev do petih let.

Neupravičen vstop v informacijski sistem

225. člen KZ

(1) Kdor neupravičeno vstopi v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v ali iz informacijskega sistema, **se kaznuje z denarno kaznijo.**

(2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.

(3) Poskus dejanja iz prejšnjega odstavka je kazniv.

(4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.

Napad na informacijski sistem

221. člen predloga novega KZ-1

- (1) Kdor vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, **se kaznuje z zaporom do enega leta.**
- (2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.
- (3) Poskus dejanja iz prejšnjega odstavka je kazniv.
- (4) Če je z dejanjem iz drugega odstavka tega člena povzročena velika škoda, se storilec kaznuje z zaporom od treh mesecev do petih let.
- (5) Kdor z namenom, da se izvrši dejanje iz prejšnjih odstavkov, poseduje, daje v uporabo, uvaža, izvaža ali drugače zagotavlja posebne pripomočke za vdor v informacijski sistem, ki niso sestavni del dovoljenih računalniških programov, se kaznuje z denarno kaznijo ali z zaporom do šestih let.**

Vdor v informacijski sistem

242. člen KZ

(Vdor v poslovni informacijski sistem)

(237. člen predloga novega KZ)

(1) Kdor **pri gospodarskem poslovanju** neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem vnese kakšen svoj podatek, ovira prenos podatkov ali delovanje informacijskega sistema, ali kako drugače vdre v informacijski sistem, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil premoženjsko škodo, se kaznuje z zaporom do treh let.

(2) Če je bila z dejanjem iz prejšnjega odstavka pridobljena velika premoženjska korist ali povzročena velika premoženjska škoda in je šlo storilcu za to, da sebi ali komu drugemu pridobi tako premoženjsko korist ali drugemu povzroči tako premoženjsko škodo, se kaznuje z zaporom do petih let.

Izdelovanje in pridobivanje pripomočkov...

Izdelovanje in pridobivanje orožja in pripomočkov,
namenjenih za kaznivo dejanje

309. člen (306. člen predloga novega KZ-1)

(1) Kdor orožje, razstrelilne snovi ali pripomočke, s katerimi se lahko napravijo, ali strupe, za katere ve, da so namenjeni za kaznivo dejanje, izdelata ali si jih pridobi ali jih hrani ali komu omogoči, da pride do njih, se kaznuje z zaporom do treh let.

(2) Kdor napravi ali komu odstopi ponarejen ključ, odpirač ali kakšen drug pripomoček za vlom, čeprav ve, da je namenjen za kaznivo dejanje, se kaznuje z zaporom do enega leta.

(3) Enako se kaznuje, **kdor z namenom izvršitve kaznivega dejanja** poseduje, izdeluje, prodaja, daje v uporabo, uvaža, izvaža ali na drug način zagotavlja **pripomočke za vdor ali neupravičen vstop v informacijski sistem.**

Izdelovanje in pridobivanje pripomočkov...

- Tako bo po **predlogu KZ-1**:
 - po **306. členu KZ-1** posedovanje (...) pripomočkov za vdor v informacijski sistem z namenom izvršitve kaznivega dejanja kaznivo **z zaporom do enega leta**;
 - po **221. členu KZ-1** posedovanje (...) pripomočkov za vdor v informacijski sistem, **ki niso sestavni del dovoljenih računalniških programov**, z namenom izvršitve dejanja vdora, prestrazanja neupravičene uporabe, spremenitve, preslikave, prenašanja, uničenja ali neupravičenega vnosa kakšnega podatka ter oviranja prenosa podatkov ali delovanja informacijskega sistema kaznivo **z denarno kaznijo ali z zaporom do šestih let**.

Nekateri vidiki uporabe tehnologij za zaščito zasebnosti

Dileme pri uporabi tehnologij za zaščito zasebnosti

- Zakrivanje identitete, kdo je pravi storilec in kdo žrtev?
- Anonimizacija
 - Tor omrežje (pravica do zasebnosti, boj proti cenzuri),
 - “zasebni” posredniški strežniki.
- Šifriranje komunikacij in nosilcev podatkov
 - zahteva po razkritju gesel in privilegij zoper samoobtožbo,
 - verodostojno zanikanje in steganografija.
- Orodja za preverjanje varnosti (*penetration testing*).
- Legitimna tehnologija je lahko tudi zlorabljena, vendar to še ni razlog za prepoved tehnologije.

Vprašanja in debata.