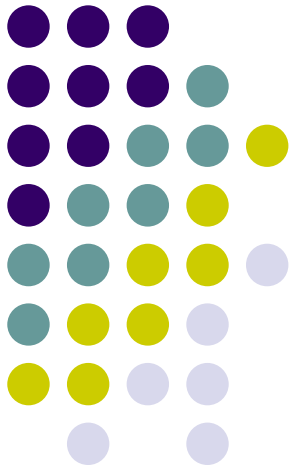
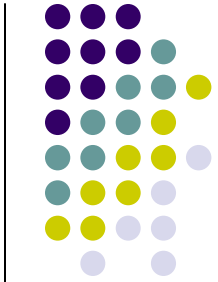
KOMPJUTERSKI KRIMINAL

Prof.dr Predag Dimitrijevic

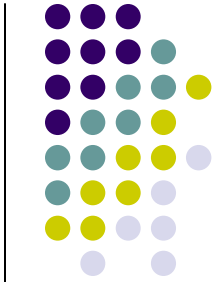


Savremena informaciona i kompjuterska tehnologija



- Savremena informaciona i kompjuterska tehnologija unela je nove i drastične **promene u sve sfere društvenog života**. Te promene su pored pozitivnih i korisnih novina donele i niz problema vezanih za pojavu i širenje kompjuterskog kriminaliteta različitih oblika, formi i vidova ispoljavanja.
- Sve te promene se mogu **svesti na sledeće**:
- - nove forme vrednosti,
- - koncentracija podataka,
- - novi ambijent delovanja,
- - nove metode i tehnike delovanja,
- - sužavanje vremenske skale delovanja,
- - širenje geografskog prostora delovanja,
- - pokretljivost,
- - stabilnost rizika.

Kompjuterski kriminal



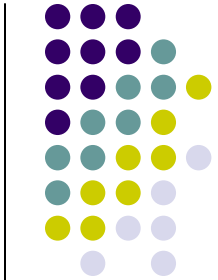
- Kompjuterski kriminal je pojava novijeg vremena
- poseban vid kriminaliteta.
- Pod kompjuterskim kriminalom obično se podrazumeva krpminalitet koji angažuje kompjuter kao sredstvo ili kao cilj izvršenja krivičnih dela.
- u osnovi reč o potojećim oblicima kriminala koji čine ljudi, a ne kompjuteri
- kriminal u vezi s kompjuterima nije samo još jedan oblik običnog kriminala, već je to opšti vid svih oblika kriminala, tako da će kako nenasilni, tako i nasilni kriminal biti vezan za kompjutere. Ubuduće neće biti korisno razdvajati nekompjuterski od kompjuterskog kriminala.

Različiti termini

- kompjuter postaje sredstvo vršenja različitih oblika nedozvoljenih, protivpravnih i društveno opasnih delatnosti.
- kompjuterski kriminalitet pod čijim zbirnim nazivom su obuhvaćeni svi ovi raznoliki oblici i forme ponašanja **nema opšte usvojenu definiciju**.
- Tako se u krivičnopravnoj literaturi za ove raznolike oblike kompjuterskog kriminaliteta upotrebljavaju različiti termini kao što su:

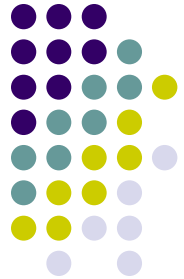
  1) zloupotreba kompjutera (computer abuse),
  2) kompjuterska prevara (computer fraud),
  3) delikti uz pomoć kompjutera (crime by computer),
  4) informatički kriminalitet,
  5) računarski kriminaliteti i
  6) tehno kriminalitet.

Ne predstavlja još uvek zaokruženu **fenomenološu kategoriju**



- Ovaj vid kriminaliteta za razliku od drugih **ne predstavlja još uvek zaokruženu** fenomenološu kategoriju te ga je nemoguće definisati jedinstvenim i precizno pojmovnim određenjem.
- Kompjuterski kriminalitet je samo opšta forma kroz koju se ispoljavaju različiti oblici kriminalne delatnosti.
- To je kriminalitet koji je upravljen protiv bezbednosti informacionih (kompjuterskih, računarskih) sistema u celini ili u njenom pojedinim delu na različite načine i različitim sredstvima u nameri da se sebi ili drugom pribavi kakva korist ili da se drugome nanese kakva šteta

Osnovne karakteristike
ili obeležja pojma kompjuterskog kriminaliteta



1. društveno opasna, protivpravna ponašanja za koja zakon propisuje krivične sankcije,
2. specifičan način i sredstvo vršenja krivičnih dela, uz pomoć ili posredstvom kompjutera,
3. poseban objekt zaštite, bezbednost računarskih podataka ili informacionog sistema u celini ili pojedinog segmenta (dela),
4. namera učinioca da sebi ili drugom na ovaj način pribavi kakvu korist (imovinsku ili neimovinsku) ili da drugome nanese kakvu štetu.

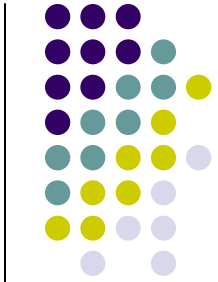
Borba protiv kompjuterskog kriminala

- Borba protiv kompjuterskog kriminala zasniva se na preventivnim i represivnim merama.
- Represivne operativno-taktičke mere su iste kao i kod drugih vidova kriminaliteta.
- Preventivne mere su specifične. One su usmerene na preduzimanje aktivnosti u cilju otklanjanja izvora. uslova, okolnosti ili propusta koji pogoduju neovlašćenom korišćenju ili zloupotrebi kompjutera.
- Preventivnim merama treba obezbediti:
- a) identifnkaciju mogućih napada na kompjuter i njihovu klasifikaciju s aspekta verovatnoće realizacije, objekta napada, načina i posledica realizacije;
- b) izbor i postavljanje odgovarajućeg mehanizma zaštite;
- v) održavanje, proveru i unapređenje postavljenog mehanizma zaštite.

Pojavni oblici kompjuterskog kriminaliteta

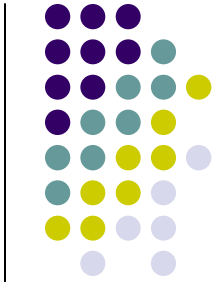
- Kompjuteri i kompjuterska tehnologija se mogu zloupotrebljavati na razne nacine, a sam kriminalitet koji se realizuje pomocu kompjutera moze imati oblik bilo kog od tradicionalnih vidova kriminaliteta, ako sto su kradje, utaje, pronevere, dok se podaci koji se neovlasceno pribavljaju zloupotrebom informacionih sistema mogu na razne nacine koristiti za sticanje protivpravne koristi.

Fenomenologija



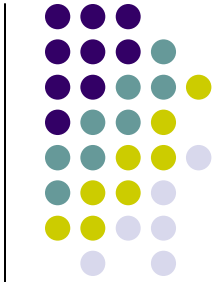
- Pojavni oblici kompjuterskog kriminaliteta su:
  1. **protivpravno koriscenje usluga**
  2. **neovlasceno pribavljanje informacija**,
  3. **kompjuterske kradje**,
  4. **kompjuterske prevare**,
  5. **kompjuterske sabotaze**
  6. **kompjuterski terorizam** i
  7. **kriminal vezan za kompjuterske mreze**.

Pojavni oblici kompjuterskog kriminaliteta



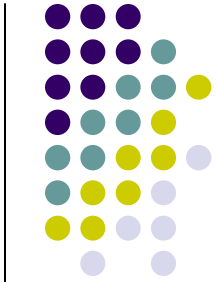
- Pojavni oblici kompjuterskog kriminaliteta mogu biti mnogobrojni, uglavnom se mogu svesti na četiri oblika:
- krađa usluga;
- informacijski kriminalitet;
- imovinski kriminalitet;
- neimovinski kriminalitet.

U teoriji krivičnog prava



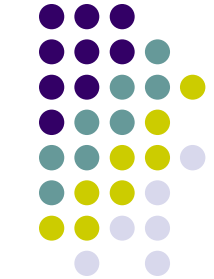
- U teoriji krivičnog prava se u oblast kompjuterskog kriminaliteta svrstavaju **različiti oblici** protivpravnog, nedozvoljenog ponašanja kao što su :
- 1. kompjuterska prevara,
- 2. finansijske krađe, prevare i zloupotrebe,
- 3. krađa dobara,
- 4. falsifikovanje podataka i dokumenata,
- 5. vandalizam,
- 6. sabotaža,
- 7. hakerisanje,
- 8. kompjuterska špijunaža i
- 9. krađa vremena.

Prevara s robom "neverovatnih" svojstava



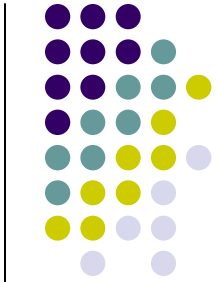
- jedan od najvecih izvora nelegalne zarade na Internetu.
- svake 44 sekunde neko postane zrtva posto se odluci da kupi robu sa cijim se "cudotvornim mogucnostima" upozna preko Interneta.
- 1400 sumnjivih sajtova samo u oblasti zdravlja, sto je rezultiralo podizanjem tuzbi protiv 18 kompanija i detaljnim istragama koje su u toku a obuhvataju jos 200 firmi u 19 zemalja sirom sveta.
- Sama cifra stete od ove neleglane trgovine nije pominjana ali ako se zna da takvi proizvodi kao recimo serija "Ljubicasta harmonija" - od kojih jedan produkt navodno uspostavlja novi nivo energije u ljudskom organizmu – kostaju izmedju 30 i 1095 dolara, lako se da izracunati koliko je to milijardi dolara svakog dana. Na vrhu liste "svemogucih" proizvoda koji se prodaju na Internetu nalaze se pilule koje omogucavaju svojim korisnicima da piju piva koliko zele, a da se ne ugoje (cena 71 dolar za 60 tableta) i pojas, koji kad se nisi u fotelji izaziva isti efekat kao 600 sklekova uradjenih u 10 min (cena 146 dolara), ljuske od jajeta ptice emu koje navodno povecavaju libido, tecnost koja masnocu iz tkiva tokom spavanja pretvara u misice, hormoni koji vracaju veru u sopstvene snage, magneti protiv nesanice, voda koja leci artritis, lekovi za lecenje SIDE , akoji dolaze iz Afrike kao resenje zagonetke zasto neke Afircke zene imaju imunitet na ovu bolest...

Kompjuterske sabotaze i kompjuterski terorizam



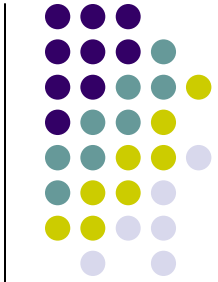
- 1997., IRA kad je sokirala englesku javnost upucivanjem pretnje da ce pored bombi, atentata i drugih oblika teroristickih akata poceti da koristi elektronske napade na poslovne i vladine kompjuterske sisteme.
- Iskustva sa Al-Quaidom pokazuju da se pripadnici ove teroristicke organizacije sluze sofisticiranim tehnikama zastite svojih kanala komunikacije na Internetu, stalno postavljaju nove web lokacije na kojima propagiraju svoje fundamentalisticke ideje, a kod nekih od uhapsnih terorista pronadjeni su kompjuteri sa sifrovanim fajlovima.

Kompjuterske mreze



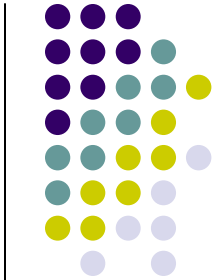
- **kao cilj napada** – napadaju se servisi, funkcije i sadrzaji koji se na mrezi nalaze. Kradu se usluge i podaci, ostecuju se ili unistavaju delovi ili celam mreza i kompjuterski sistemi, ili se ometaju funkcije njihovog rada. U svakom slucaju cilj pocinilaca je mreza u koju se ubacuju malware, vrse DOS napadi...
- **kao sredstvo ili alat** - Danas modrni kriminalci koriste sve vise kompjuterske mreze kao orudja za realizaciju svojih namera. Koriscenje pvog novog orudja narocito je popularno kod decje pornografije, zloupotrebe intelektualne svojine ili online prodaje nedozvoljene robe (droga, ljudskih organa, nevesta..)
- **kao okruzenje u kome se napadi realizuju**. Najcesce to okruzenje sluzi za prikrivanje kriminalnih radnji, kao sto to beoma vesto uspevaju da urade pedofili, a ni drugi kriminlci nisu nista manje uspesni. Naravno postoje i druge uloge, kao sto je npr., koriscenje mreze kao simbola zastrasivanja, uplitanja, koje su nekad vise izrazeme kod kompjuterskog nego kod cyber kriminala.

Cyber kriminal **zavisno od tipa pocinjenih dela moze biti:**



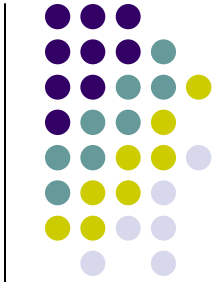
- **Politicki**:
  - cyber spijunaza i cyber sabotaza, (Spijunaza i sabotaza u svetu racunara)
  - haking, (**Osnovi bezbednosti na Internetu** , **Osnovi zastite od kompjuterskih virusa, crva i 'trojanaca'**)
  - cyber terorizam (Asimetricni virtuelni rat – internet kao oruzje terorista)
  - cyber ratovanje (**Implikacije eventualnog oruzanog sukoba SAD i Iraka na Cyber prostor**)

Cyber kriminal **zavisno od tipa pocinjenih dela moze biti:**



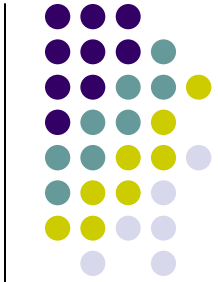
- **Ekonomski**:
- cyber prevare ('Nigerijska podvala' ili pranje novca-, **Osnovni saveti i pravila za sprecavanje prevara pri trgovini hartijama od vrednosti na Internetu, kao vidu kompjuterskog kriminaliteta**, tekst "Socijalni inzinjering - **Sprecavanje zloupotrebe Interneta i nanosenja stete korisniku**) ,
- haking (**Osnovi bezbednosti na Internetu** , **Osnovi zastite od kompjuterskih virusa, crva i 'trojanaca'**, **E-mail od onih kojima se veruje**),
- kradja internet vremena, kradja internet usluga (**Sprecavanje zloupotrebe Interneta i nanosenja stete korisniku**)
- piratstvo softvera, mikrocipova i BP,
- cyber industrijska spijunaza , (Spijunaza i sabotaza u svetu racunara)
- spam.
- proizvodnja i distribucija nedozvoljenih stetnih sadrzaja kao sto su decja pornografija, pedofilija, verske sekte, sirenje rasistickih , nacistickih i slicnih ideja i stavova (Dzihad preko Interneta**)**
- zloupotreba zena i dece.
- manipulacija zabranjenim proizvodima , supstancama i robama – drogama, ljudskim organima, oruzjem.
- povrede cyber privatnosti – nadgledanje e poste, prisluskivanje, snimanje "pricaonica", pracenje e-konferencija, prikacinjanje i analiza spijunskih softvera i "cookies" (Zastita od spyware softvera - **Sprecavanje zloupotrebe Interneta i nanosenja stete korisniku**)

POJAM KOMPJUTERSKOG KRIMINALITETA



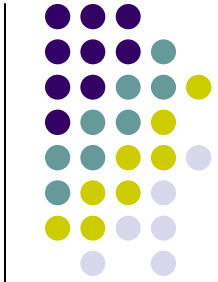
- Definisanje kompjuterskog kriminaliteta je izuzetno teško, jer (razloga):
- 1. reč je o relativno novom obliku kriminalnog ponašanja, koji se još nije u potpunosti izdiferencirao u odnosu na druge vidove kriminaliteta,
- 2. kompjuterski kriminalitet ispoljava veliku fenomenološku raznovr-snost, koja se teško može obuhvatiti jednom definicijom,
- 3. nisu tako retka zakonodavstva koja poznaju kompjuterske delnkte kao posebna krivična dela, nauka se ne može u određivanju pojma kompjuterskog krimnnaliteta oslanjati u većoj meri na pozitivnu krnvičnopravnu legislativu.

Način izvršenja



- Način izvršenja ovih delikata zasniva se na upotrebi kompjutera, pri čemu samo korišćelje računara može biti ispoljeno kao celovit modus opcrandi, ili kao jedan njegov segment.
- Kompjuter može biti i osnovno sredstvo izvršenja ovih krivičnih dela, a potrebno je pored toga da je ostvarena i neka u krivičnopravnom smislu kažnjiva posledica, s tim što posledica može biti ispoljsna na samim kompjuterima, informatičkoj ili komunikacijskoj mreži.

Posledice kompjuterskog kriminaliteta



- **Stete** nastale vrsenjem kompjuterskih delikata, zavisno od pojavnog obilaka kompjuterskog kriminaliteta, mogu se podeliti na:
  1. **finansijske** – koje mogu da nastanu kada ucinilac vrsi delo u cilju sticanja protivpravne imovinske koristi, pa tu koristi za sebe ili drugo, zaista i stekne, ili je ne stekne, ali svojim delom objektivno pricini odredjenu stetu, ili kada ucinilac ne postupa radi sticanja koristi za sebe ili drugog, ali objektivno ucini finansijsku stetu.
  2. **nematerijalne** – koje se ogledaju u neovlascenom otkrivanju tudjih tajni , ili drugom "indiskretnom stetnom postupanju"
  3. **kombinovane** – kada se otkrivanjem odredjene tajne , ili povredom autorskog prava, putem zloupotrebe kompjutera ili informaticke mreze narusi neciji ugled, odnosno povredi moralno pravo a istovremeno prouzrokuje i konkretna finansijska steta.

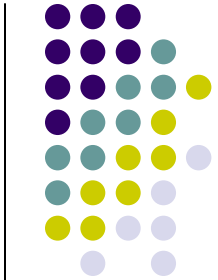
Pojam

- Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog dela
- ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krnvičnopravnom smislu relevantna posledica.
- Kompjuterski kriminalitet je takodje protivpravna povreda imovine kod koje se racunarski podaci s predumisljajem menjaju (manipulacija racunara), razaraju (racunarska sabotaza), ili se koriste zajedno sa hardverom (kradja vremena).

KARAKTERISTIKE UČINILACA

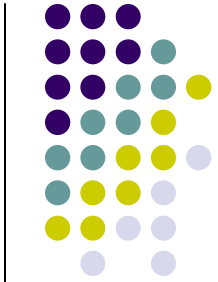
- Ne može se govoriti o jedinstvenom profilu učinilaca kompjuterskog kriminaliteta,
- oni se svrstavaju u različite kategorije prema pojavnim oblicima dela koja čine, ali i prema motivima, koji ih pokreću u vršenju kriminalnih aktivnosti.
- Učinioci ovih dela se mogli podeliti na:
- zlonamerne, koji mogu da deluju radi ostvarenja imovinske koristi, ili samo u cilju nanošenja štete i
- na učinioce koji nisu motivisani ne ostvarenjem koristi, niti prouzrokovanjem štetnih posledica, već jednostavno traže zadovoljstvo u neovlašćenom prodiranju u neki dobro obezbeđen informacioni sistem. To su tzv. hakeri *(hackers),* koji koristeći svoje računarsko znanje, upadaju u tuđe kompjuterske sisteme.

Hakeri



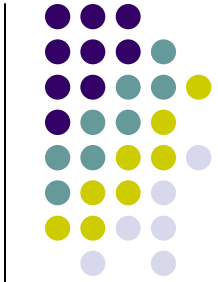
- Ovi učinioci predstavljaju kompjuterske entuzijaste, koji provaljujući u dobro čuvane informatičke sisteme iživljavaju svoju strast za avanturama po tzv „informacionim autostradama" u specifičnom cyber-spacesu.
- Oni su često pravi „kompjuterski zavisnici" koji čak ponekad nemaju pravi kontakt s realnošću, već prvenstveno obitavaju u svom „virtuelnom svetu". Oni vrhunsko zadovoljstvo nalaze u samom činu provaljivanja u višestruko obezbeđene informacione sisteme i što su kompjuterski sistemi bolje čuvani, to je za hakere veći izazov da se upuste u za njih spektakularno savladavanje „kripto-grafskih brava". Zato su na meti ovih učinilaca. često najbolje obezbeđeni informacioni sistemi kao što su kompjuterske mreže vlada savremenih država, ili vojnih laboratorija, pa i u kompjuterske sisteme Pentagona.
- Hakeri mogu svesno ili nesvesno da prouzrokuju ogromne štete. Oni su prema svom profesionalnom opredeljenju najčešće programeri kompjutera, visokoobrazovani informatičari, a ponekad je reč o osobama koje su svoju veštinu i znanje stekli baveći se kompjuterima iz hobija. To su veoma inteligentni učinioci a jedina prava zaštita od njihovih provala je jačanje krpptografskih spstema zaštite, uz strožu kriminalnu politiku prema ovakvim učiniocima
- Oni, nezavisno od motiva koji ih pokreću, realno predstavljaju velnku opasnost, naro-čito u situacijama kada se upuštaju u rizične informatičke avanture u tako osetljivim područjima kao što su nacionalna bezbednost, industrija naoružanja, satelitska tehnologija itd.

Zlonamerni učinioci kompjuterskih delikata



- Zlonamerni učinioci kompjuterskph delikata najčešće su motivisani koristoljubljem.
- Oko 80% delikvenata čini delo prvi put, a 70% je zaposleno više od pet godina u oštećenom preduzeću.
- njihovo starosno doba je između 19 i 30 godina, pretežno su muškog pola, veoma su inteligentni; imaju uglavnom više godina radnog iskustva i važe kao savesni radnici koji prilikom obavljanja radnih zadataka ne prouzrokuju nikakve probleme, često su tehnički kvalifikovaniji nego što to zahteva radno mesto na koje su raspoređeni;
- ovi učinioci sebe po pravilu ne smatraju kradljivcima ili uopšte kriminalcima, već samo pozajmljivačima.

Koristoljubivi kompjuterski kriminalitet

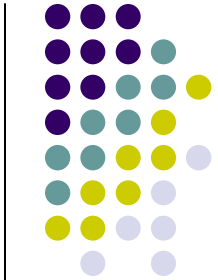


- Koristoljubivi kompjuterski kriminalitet veoma je čest u bankarstvu, finansijskim korporacijama i osiguravajućim društvima.
- Statistički podaci o učiniocima kompjuterskih delikata u oblasti bankarskih poslova ukazuju na najčešće profesije učinilaca: 25% čine osobe sa specijalnim ovlašćenjima sa odgovornostnma u informatičkim sistemima, 18% programeri, 18% službenici koji raspolažu terminalima, 16% blagajnici. 11% operateri-informatičari i u 12% slučajeva učinioci su lica van oštećenih korporacija, u šta su uključeni i korisnici usluga.

KOMPJUTERSKI KRIMINALITET U UPOREDNOM KRIVIČNOM PRAVU

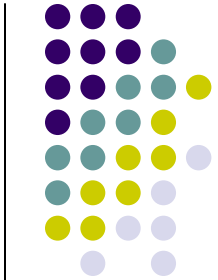
- Budući da **preventivne mere** (opšteg i specijalnog karaktera) često **nisu dovoljne** niti jedine mere kojima se društvo suprotstavlja naraslim i nabujalim oblicima i vidovima zloupotrebe komjutera u različite svrhe, to je logično da sva savremena krivična zakonodavstva u sistemu inkriminacija poznaju jedno ili više kompjuterskih (računarskih ili informatičkih ili tehno) krivičnih dela za koja su propisane različite vrste i mere krivičnih sankcija.
- Tako, iako **Nemački krivični zakonik** (*Schonke-Schroder, Strafgesetzbuch, Munchen, 1978. godine*) ne poznaje kompjuterska krivična dela, to ne znači da ova protivpravna, nedopuštena ponašanja nisu inkriminisana. Naime, u Nemačkoj je 1986. godine donet poseban Krivični zakon za suzbijanje privrednog kriminaliteta koji predviđa niz kompjuterskih krivičnih dela i to: kompjutersku špijunažu u čl. 202a., kompjutersku prevaru u čl. 263a., falsifikovanje podataka u čl. 269., obmanu u pravnom prometu pri obradi podataka u čl. 270., promenu podataka u čl. 302a. i kompjutersku sabotaža u čl. 303a.

KOMPJUTERSKI KRIMINALITET U UPOREDNOM KRIVIČNOM PRAVU



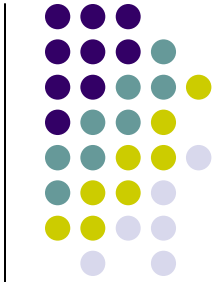
- **Krivični zakonik Austrije** (*E. Foregger-E. Serini, Strafgesetzbuch, Wien, 1989. godine*) predviđa kompjutersko krivično delo u čl. 126a. Ono se zove oštećenje podataka.
- **U Velikoj Britaniji** je 1990. godine donet poseban Zakonik o zloupotrebi kompjutera. Ovaj zakonik predviđa niz krivičnih dela vezanih za zloupotrebu kompjutera i drugih informacionih sistema za koju se propisane veoma stroge kazne (*Martin Wasik, The computer misuse act, The Criminal Review, 1990. godine, str. 767*).

KOMPJUTERSKI KRIMINALITET U UPOREDNOM KRIVIČNOM PRAVU



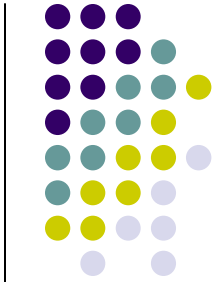
- **Krivični zakonik Makedonije** (Služben vesnik na Republika Makedonija, Skopje, broj 37/1996) poznaje u čl. 251. kompjutersko krivično delo pod nazivom. Upad u kompjuterski sistem.
- Na sličan način postupa i **Krivični zakonik Republike Srpske** (Službeni glasnik Republike Srpske, Banja Luka, broj 22/2000) koji poznaje identično krivično delo pod nazivom: Upad u kompjuterski sistem u čl. 260.
- **Krivični zakonik Republike Slovenije** (*B. Penko, K. Strolig, Kazenski zakonik z uvodnimi pojasnili, Ljubljana, 1999.*) poznaje sledeća krivična dela i to : Protivzakoniti ulaz u zaštićenu računarsku bazu podataka u čl. 225 i Upad u računarski sistem u čl. 242.
- **Krivični zakon Republike Hrvatske** (*Narodne novine Republike Hrvatske, Zagreb, broj 110/1996*) u čl. 223. poznaje krivično delo pod nazivom: Oštećenje i upotreba tuđih podataka (koje se odnosi na automatski obrađene podatke ili računarske programe).
- **Krivični zakonik Ruske federacije** (*J. I. Skuratov, V. M. Lebedov, Kommentarii k uglavnom u kodeksu Rossijskoj federaciji, Moskva, 1996.*) poznaje više kompjuterskih krivičnih dela u posebnoj glavi 23. koja nosi naziv: Krivična dela u sferi kompjuterske informacije. Ovde su propisana sledeća krivična dela: Protivpravni pristup kompjuterskoj informaciji u čl. 272., Pravljenje, korišćenje i širenje štetnih računarskih programa u čl. 273. i Povreda propisa o eksploataciji računara, računarskih sistema ili njihovih mreža u čl. 274.

KOMPJUTERSKA KRIVIČNA DELA



- Kompjuterska krivična dela uvedena su **Krivnčnim zakonom Srbije** 2005. godine. koja su u Glavi 27 predviđena kao „krivična dela protnv računarskih podataka" (čl. 298-304). Osim toga, u Okružnom javnom tužilaštvu u Beogradu 2005. godine je osnovano **posebno odeljenje za borbu protiv vosokotehnološkog kriminala.**
- Krivični zakon daje zakonske definicije koje se odnose na kompjuterska krivičia dela:
- „Računarski podatak" predstavlja informacija, znanje, činjenicu, koncept ili naredbu koja se unosi, obrađuje ili pamti ili je uneta, obrađena ili zapamćena u računaru ili računarskoj mreži.
- „Računarska mreža" je skup međusobno povezanih računara koji komuniciraju razmenjujući podatke.
- „Računarski program" je uređeni skup naredbi koji služe za upravljanje radom računara. kao i za rešavanje određenog zadatka pomoću računara.

Zakonske definicije koje se odnose na kompjuterska krivičia dela:



- „Računarski virus" je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka.
- „Ispravom" se smatra svaki predmet koji je podoban ili određen da služi kao dokaz kakve činjenice koja ima značaj na pravne odnose, kao i računarski podatak,
- „Pokretna stvar" je svaka proizvedena ili sakupljena energija za davanje svetlosti, toplote ili kretanja, telefonski impuls, kao i računarski podatak i računarski program.

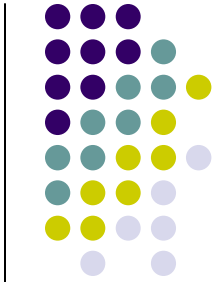
Krivični zakon predviđa sledeća krivična dela protiv bezbednosti računarskih podataka:

- **Oštećenje računarskih podataka i programa** (čl. 298). Ko neovlašćeno izbriše, izmeni, ošteti. prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program, kazniće se novčanom kaznom ili zatvorom do jedne godine.
- Ako prouzrokovana šteta prelazi četristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do tri godine.
- Ako prouzrokovana šteta prelazi milion i petsto hiljada dinara, učinilac će se kaznnti zatvorom od tri meseca do pet godnna.
- Uređaji i sredstva kojima je učinjeno ovo krivično delo, ako su u svojini učinloca, oduzeće se.

Krivična dela protiv bezbednosti računarskih podataka:

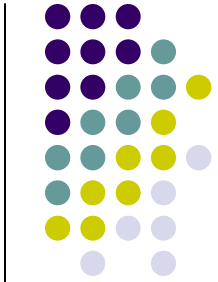
- **Računarska sabotaža** (čl. 299). Ko unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte, kazniće se zatvorom od šest meseci do pet godnna.
- **Pravljenje i unošenje računarskih virusa** (čl. 300). Ko napravi računarskn virus u nameri njegovog unošenja u tuđ računar ili raču-narsku mrežu, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili zatvorom do dve godine. Uređaj i sredstva kojima je učinjeno ovo krivično delo oduzeće se.

Krivična dela protiv bezbednosti računarskih podataka:



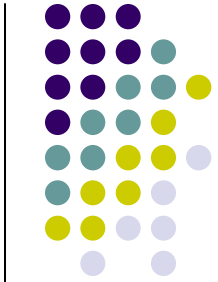
- **Računarska prevara** (čl. 301). Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u namern da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje pmovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine.
- Ako pribavljena imovinska korist prelazi iznos od četiristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od jedne do osam godina.
- Ako pribavljena imovinska korist prelazi iznos od milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od dve do deset godina. Ko ovo delo učini samo u nameri da drugog ošteti, kazniće se novčanom kaznom ili zatvorom do šest meseci.

Krivična dela protiv bezbednosti računarskih podataka:



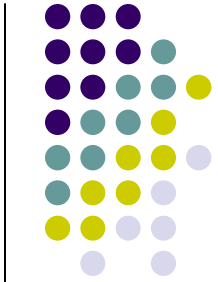
- **Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka** (čl. 302). Ko se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom ka-znom ili zatvorom do šest meseci.
- Ko upotrebi ovako dobijen podatak, kazniće se novčanom kaznom ili zatvorom do dve godine.
- Ako je došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade prenosa podataka ili mreže ili su nastupile druge teške posledice, učinilac će se kazniti zatvorom do tri godine.

Krivična dela protiv bezbednosti računarskih podataka:



- **Sprečavanje i ograničavanje pristupa javnoj računiarskoj mreži** (čl. 303). Ko neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži, kazniće se novčanom kaznom ili zatvorom do jedne godine. Ako delo učini službeno lice u vršenju službe, kazniće se zatvorom do tri godine.
- **Neovlašćeno korišćelje računara ili računarske mrsže** (čl. 304). Ko neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili zatvorom do tri meseca. Gonjenje za ovo krivično delo preduzima se po privatnoj tužbi.

Cuvanje elektronske baze podataka

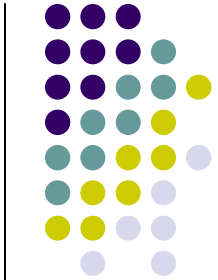


- Kako sacuvati vazne elektronske podatke od gubljenja, unistenja, zloupotreba ili bilo koje druge vrste neadekvatnog koriscenja, postaje sve ozbiljniji problem. Resenje sa podzemnim, dobro obezbedjenim, sklonistima deluje realno, ali... bekap server na Mesecu deluje, u pravom smislu reci, zilvernovski?!

Kako se odbraniti od ostecenja ili gubitka vaznih podataka i dokumentacije?

- Velike kompanije poput IBM-a ulazu novac i resurse u razvijanje ovakvih sistema, koji postaju sve brzi, pouzdaniji i imaju sve veci kapacitet.
- Medjutim, posle teroristickog napada u Njujorku, veliki broj firmi je nepovratno izgubio sve svoje podatke, i to iz jednostavnog razloga – u rusenju objekata nastradale su i sve bekap kopije.
- kakav znacaj imaju svi bekap serveri i silni terabajti podataka ako u slucaju ovakvog ili slicnog dogadjaja nastradaju i ti uredjaji.
- Zbog toga su ideje o cuvanju podataka u atomskom sklonistu, ili cak na povrsini Meseca, postale interesantne mnogim kompanijama koje sebi ne mogu da dozvole ovakvu vrstu gubitka.

Iron Mountain

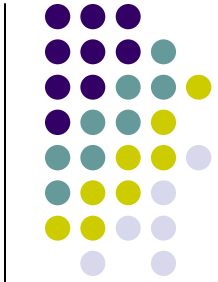


- Kompanija Iron Mountain je osnovana 1951. godine, kada je otkupljen veliki napusteni rudnik u toj oblasti. Objekat sadrzi veliki broj nivoa (rudarskih horizonata) sa prostranim razgranatim hodnicima, sto se pokazalo kao idealno mesto za stvaranje neke vrste podzemne baze.
- Rudnik je adaptiran, i u vreme Hladnog rata je sluzio za slicne stvari za koje sluzi i danas – brojne firme i ustanove su u prostorijama ove podzemne baze odlagale svoje papirne arhive, proizvode ili predmete od vrednosti. Sa sve vecim prisustvom racunara u savremenom poslovanju i u okolnostima kada pojedine firme u potpunosti ukidaju papirno poslovanje, ova kompanija je svoj podzemni objekat dobrim delom preorijentisala, te on sada uglavnom sluzi za arhiviranje elektronskih dokumenata. U kilometre podzemnih hodnika uneti su racunari, monitori, bekap serveri itd, a citav podzemni data-centar lici na pravi mali grad sa cak 2000 zaposlenih.

Iron Mountain

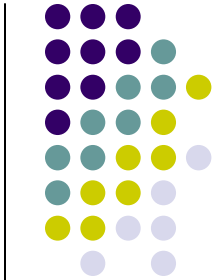
- Samo jedna kompanija koja je korisnik ove usluge nedeljno prosledi na arhiviranje preko dva miliona e-mail i instant poruka, koje neprekidno teku kroz dve zakupljene linije. Na specijalni zahtev klijenta, po prispecu na servere podzemnog centra, prave se dodatne dve kopije podataka na WORM diskovima. Ovo su posebni mediji na koje se elektronski podaci mogu upisati samo jednom, a citati mnogo puta.
- Ovakav pristup arhiviranju zahtevaju vazeca zakonska pravila u SAD jer se jedino na taj nacin obezbedjuje pravna valjanost arhiviranih podataka u eventualnim sudskim sporovima.

Iron Mountain



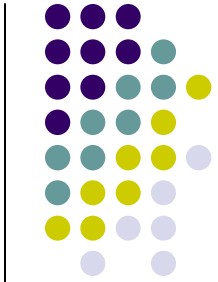
- U podzemnom racunskom centru grupa servera na prvoj liniji prihvata prispele podatke i na njima primenjuje pravila o arhiviranju koja je postavio klijent. Ovo se odnosi na dodeljivanje tagova koji odredjuju nacin procesiranja i kasnijeg opozivanja podataka, a primenjuje se „digitalni otisak prsta" kao i ostali neophodni postupci.
- Nakon toga se podaci upisuju na hard diskove, a kasnije, prema programiranom rasporedu, na sisteme sa trakama. Brisanje podataka koji vise nisu potrebni odigrava se posle unapred odredjenog roka koji postavljaju klijenti ili se oni brisu rucno. Sistem stvara indeks arhiviranih elektronskih dokumenata, omogucavajuci pretrazivanje uz pomoc bilo kojeg savremenog Web pretrazivaca.
- Cena usluge koju pruza kompanija krece se od 12 USD mesecno po jednom gigabajtu, a kako bude rasla potraznja i budu prosirivani kapaciteti, srazmerno ce padati i visina troskova.

"earthDATAsafe"



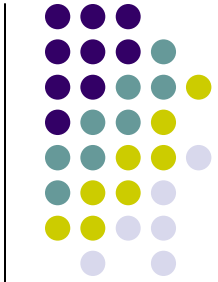
- Evropljani mogu da se pohvale jednim slicnim objektom koji se nalazi u okolini grada Kapfenberga u Austriji. Objekat je po svojoj nameni i nacinu funkcionisanja veoma slican prethodnom, mada je trenutno fizicki znatno manji, sa manjim brojem zaposlenih i tek je nedavno poceo s radom.
- Objekai i sistem nose naziv "earthDATAsafe" a ceo kompleks je zvanicno otvoren u novembru 2003. godine i jos uvek je dobar deo racunarske strukture u fazi postavljanja i probnog rada. Pokretac ovog projekta je kompanija Daimler Chrysler Consult Graz Gmbh, sa svojim partnerima a korisceni su rezultati istrazivanja koja je vrsila nemacka firma OTRAG (Orbital Transport Group) u svojim tajnim laboratorijama u kongoanskoj dzungli jos sredinom sedamdesetih godina XX veka. Kompanija UIA iz Nemacke obezbedjuje sirokopropusne i bezbedne linkove, SUN Microsystems se stara o hardverskoj infrastrukturi, dok je Oracle obezbedio baze podataka velikih mogucnosti i performansi.

TransOrbital

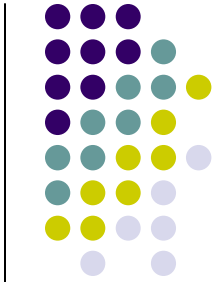


- Pokusavajuci da pronadje sto bezbednije mesto za smestanje digitalnih arhiva, kompanija TransOrbital (www.transorbital.net) iz Kalifornije ponudila je nesvakidasnje resenje – smestanje servera s podacima na Mesecu! To deluje kao veoma bezbedno mesto jer je malo verovatno da ce ruka zlonamernika dospeti tako daleko.
- Mnogi su skepticni u vezi s isplativoscu ove ideje i postavljaju pitanje da li ima smisla cuvati vazne elektronske podatke cak na Mesecu.
- Kompanija TransOrbital ima spisak klijenata koji su spremni da plate cuvanje vaznih finansijskih, tehnoloskih i vojnih podataka na ovaj nacin. Da bi sistem funkcionisao kako se ocekuje, potrebno je da se razviju bolji protokoli za prenos podataka usmerenim laserskim snopovima. Postojeci standardi koje je postavila laboratorija Jet Propulsion ne zadovoljavaju ocekivani intenzitet saobracaja.

kucni korisnici

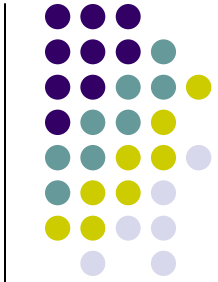


- U vreme kada cak i kucni korisnici sve vise zamenjuju papirne dokumente digitalnim, vaznost bekapa postaje sve veca. Kucni korisnici ce ovaj problem lako resiti uz pomoc nekoliko CD ili DVD diskova, dok kompanije moraju da primene strateski nacin razmisljanja.
- Veliki broj kucnih korisnika koristi vec osmisljene, funkcionalne sisteme za cuvanje podataka preko interneta kojima raspolazu velike grupacije kao sto su Yahoo (G-mail), Mail.ru, Google i slicne.
- Sistemi su zasticeni od napada hakera i raspolazu najazurnijim antivirusnim programima za zastitu podataka. Naime, svaka od njih je otvorila tzv. mail servis na kome svaki posetilac, uz veoma uproscenu proceduru otvara svoje postansko sanduce kapaciteta najmanje 1.000 mega bajta, koje se moze otvoriti samo uz sifru, odnosno poseban password, koji korisnik bira sam. Broj takvih postanskih sanducica je neogranicen ali svako mora da nosi posebno ime i da ima poseban password. Oni su besplatni. Sem toga, neki od pomenutih mail servisa su opremljeni dodatnim programima za proveru koji se ukljucuju automatski kadgod sistem "zakljuci" da postoji sumnja u identitet korisnika postanskog sanduceta.



- Najsigurnije je, kao sto je vec i naglaseno, narezati podatke na CD ili DVD i izabrati skrovito i sigurno mesto za njihovo cuvanje (mozda cak i u sefu neke banke)!

Kompjuterski kriminal



HVALA NA PAŽNJI!