ВИСОКОТЕХНОЛОШКИ КРИМИНАЛИТЕТ

Доц.др. Миле Шикман
Управа за полицијско образовање
МУП Републике Српске

ТЕМЕ ЗА ОБРАДУ

- ПОЈАМ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА
- КАРАКТЕРИСТИКЕ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА
- НЕКИ ОСНОВНИ ПОЈАВНИ ОБЛИЦИ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА
  - ОРГАНИЗОВАНИ ВИСОКОТЕХНОЛОШКИ КРИМИНАЛИТЕТ
- ОТКРИВАЊЕ И ДОКАЗИВАЊЕ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА
- ПРЕВЕНЦИЈА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА

ПОЈАМ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА (ВТ)

- Терминологија
  - Високотехнолошкир криминалитет
  - Компјутерски криминалитет
  - Сајбер криминалитет
  - Кибернетички криминалитет
  - Злоупотреба компјутера, компјутерска превара, информатички криминал, техно криминал и другу.
- Високотехнолошки криминалитет представља друштвено опасну појаву за чије се остварење учинилац користи знањима високотехнолошке (компјутерске, информатичке) технологије, тако што се компјутерски систем схваћен у најширем смислу (хардвер, софтвер, њихово јединство; један компјутер или мрежа компјутера), користи као средство или као објект криминалног напада или и једно и друго.

ПОДЕЛА

- најопштија подела (*Pavan Duggal*)
  - високотехнолошки криминалитет против *личности*
  - високотехнолошки криминалитет против *добара*
  - високотехнолошки криминалитет против *владе*
- традиционална подела криминалитета
  - високотехнолошки општи криминалитет
  - високотехнолошки привредно-економски криминалитет
  - високотехнолошки организовани криминалитет
  - крађа услуга

КЛАСИФИКАЦИЈА У ЗАВИСНОСТИ ОД ТИПА УЧИЊЕНОГ ДЕЛА

- Политички:
  - cyber шпијунажа и cyber саботажа, (шпијунажа и саботажа у свету рачунара)
  - хакинг, (Основи безбедности на Интернету , Основи застите од компјутерских вируса, црва и 'тројанаца')
  - cyber тероризам (Асиметрични виртуелни рат – интернет као оружје терористa)
  - cyber ратовање (Импликације евентуалног оружаног сукоба САД и Ирана на cyber простор)

- Економски:
  - cyber преваре ('Нигеријска подвала' или прање новца, превара при трговини хартијама од вредности на Интернету)
  - хакинг
  - крађа интернет времена, крађа интернет услуга
  - пиратство софтвера, микроципова и БП,
  - cyber индустријска шпијунажа, спам.
  - производња и дистрибуција недозвољених штетних садржаја као сто су дечја порнографија, педофилија, верске секте, ширење расистичких , нацистичких и сличних идеја и ставова (џихад преко Интернета)
  - злоупотреба жена и деце.
  - манипулација забрањеним производима , супстанцама и робама – дрогама, људским органима, оружјем.
  - повреде цубер приватности – надгледање е поште, прислушкивање, снимање "причаоница", праћење е-конференција, прикацињање и анализа шпијунских софтвера и “cookies”

ЕТИОЛОШКА ДИМЕНЗИЈА

- све већа заступљеност компјутерских технологија
- укљученост компјутерских технологија у приватни живот људи
- повезаност пословних активности са коришћењем савремених технологија
- све већа тенденција коришћења савремених технологија
- коришћење савремених технологија при вршењу других кривичних дјела (нпр. привредно-економског криминалитета)
- социјални инжињеринг, односно активна манипулација навођења људи да одају информације о себи.

Све те промене се могу свести на следеће:
-нове форме вредности,
-концентрација података,
-нови амбијент деловања,
- нове методе и технике деловања,
- сужавање временске скале деловања,
- ширење географског простора деловања,
- покретљивост,
- стабилност ризика.

КОМПЈУТЕР КАО...

- као средство криминалног дјеловања
  - компјутером се остварује радња извршења (средство извршења)
- као објект криминалног напада
  - компјутерски хардвер
  - комјутерских софтвер
  - подаци
- и једно и друго
  - и средство извршења и објекат извршења

Компјутер може бити и основно средство извршења ових кривичних дела, а потребно је поред тога да је остварена и нека у кривичноправном смислу кажњива последица, с тим што последица може бити испољсна на самим компјутерима, информатичкој или комуникацијској мрежи.

КАРАКТЕРИСТИКЕ

- *специфичности начина извршења* - радњу компјутерских кривичних дела карактерише читав низ специфичности у односу на до сада познате форме криминалитета
- *мањи је значај просторних и временских оквира у случајевима компјутерског криминалитета* - просторне и временске релације имају сасвим други значај и вредности у односу на друге врсте криминалитета
- *неопходна су специјална знања како за извршење тако и за откривање компјутерског криминалитета* – ова знања зависе од врсте криминалног напада
- *проблем доказивања кривичних дела компјутерског криминалитета*
- *велика тамна бројка кривичних дела из области компјутерског криминалитета* - постоји процена да се мање од 1% компјутерских проневера открије, а да више од 90% свих случајева компјутерског криминалитета остаје необјављено

ФЕНОМЕНОЛОШКА ДИМЕНЗИЈА –

Не представља заокружену феноменолошку категорију, те још увек није дефинисања његова статика, динамика и типологија

1) *Компјутерске преваре* су облик превара које се врше уз помоћ компјутера у намери прибављања себи или другоме противправне имовинске користи. Код компјутерских превара радња учиниоца није усмерена ка другом лицу како би се довело у заблуду, већ ка компјутеру.
2) *Проваљивање у туђе компјутерске системе* састоји се у онеспособљавању система заштите компјутера после чега се врши неовлашћени упад у туђи информациони систем.

3) *Крађа информација* се остварује непосредним приступом компјутеру који је објект напада или носиоцима информација (дисковима са информацијама). Посебни облик крађа информација су компјутерске шпијунаже.

4) *Крађа компјутерских услуга* представља неовлашћену употребу (односно злоупотребу) компјутера тако што се у току радног времена, на службеном компјутеру, обављају приватни послови и на тај начин остварује имовинска корист. Овај облик компјутерских злоупотреба се другачије назива и *крађа компјутерског времена*.

5) *Пиратерија у области компјутерских софтвера и других компјутерских производа*. Пиратерија у области компјутерских софтвера представља илегално копирање оригиналних компјутерских програма и њихову неовлашћену продају. Поред пиратерије у области софтвера, нису ретки случајеви *пиратерије у области компјутерских компоненти*.

6) *Компјутерска саботажа* је вид компјутерског криминала којим се врши напад на компјутерску опрему, софтвере и датотеке података како би се оштетиле или уништиле, односно како би се трајно или привремено онеспособио појединi компјутер или компјутерски центар у целини.

- комјутерски вирус и црви
- тројански коњ
- програмска или логичка бомба
- прикривени улаз

7) *Компјутерски тероризам* се испољавао, пре свега, у облику бомбашких напада на значајне државне или војне компјутерске центре или на фабрике компјутерског хардвера и софтвера. Терористичке организације користе Интернет сајтове за ширење својих идеја и врбовање младих.

8) *Криминал повезан са Интернетом*. Интернет мрежа користи се за неовлашћени упад у туђе компјутерске системе како би се остварили криминални циљеви које је себи поставио криминалац, нпр., компјутерски *haking* (неовлашћено разгледање података и повреда приватности); компјутерска саботажа (уништење, измена података и софтвера, уграђивање деструктивних програма итд.); компјутерска шпијунажа (крађа или копирање података), компјутерски тероризам итд.

ОБЛИЦИ КРИМИНАЛИТЕТА ПРЕКО ИНТЕРНЕТА

- *Преваре на Интернету*
- *Преваре приликом плаћања преко Интернета*
- *Ширење дечије порнографије* (и порнографије уопште)
- *Ширење разних облика организованог криминалитета*
- *Разни облици угрожавања личне сигурности*

ПРЕВАРА С РОБОМ "НЕВЕРОВАТНИХ" СВОЈСТАВА

- један од највећих извора нелегалне зараде на Интернету.
- сваке 44 секунде неко постане жртва посто се одлучи да купи робу са чијим се “чудотворним могућностима" упозна преко Интернета.
- 1400 сумњивих сајтова само у области здравља, што је резултирало подизањем тужби против 18 компанија и детаљним истрагама које су у току а обухватају још 200 фирми у 19 земаља широм света.
- Сама цифра штете од ове нелеглане трговине није помињана али ако се зна да такви производи као рецимо серија "Љубичаста хармонија" - од којих један продукт наводно успоставља нови ниво енергије у људском организму – коштају између 30 и 1095 долара, лако се да израчунати колико је то милијарди долара сваког дана. На врху листе "свемогућих" производа који се продају на Интернету налазе се пилуле које омогућавају својим корисницима да пију пива колико желе, а да се не угоје (цена 71 долар за 60 таблета) и појас, који кад се ниси у фотељи изазива исти ефекат као 600 склекова урађених у 10 мин (цена 146 долара), љуске од јајета птице чему које наводно повећавају либидо, течност која масноћу из ткива током спавања претвара у мисиће, хормони који враћају веру у сопствене снаге, магнети против несанице, вода која лечи артритис, лекови за лечење СИДЕ , а који долазе из Африке као решење загонетке зашто неке Афирчке зене имају имунитет на ову болест...

ВИСОКОТЕХНОЛОШКИ ОРГАНИЗОВАНИ КРИМИНАЛИТЕТ

- Информацијске и комуникацијске технологије (*Informacion and Communication Technology - ICT*) дају нови инструменти за извршење старих врста криминалитета, као и средства и тржишта за нове врсте криминалитета.
- Та нова технологија може утицати и на структуру криминалних организација и управљање предузећа која се баве криминалом, при чему друштва и предузећа са напредном ICT прате логику мреже, а не ону јасних хијерархија

ЕЛЕМЕНТИ БИЋА КРИВИЧНОГ ДЕЛА

- друштвено опасна, противправна понашања за која закон прописује кривичне санкције,
- специфичан начин и средство вршења кривичних дела, уз помоћ или посредством компјутера,
- посебан објект заштите, безбедност рачунарских података или информационог система у целини или појединог сегмента (дела),
- намера учиниоца да себи или другом на овај начин прибави какву корист (имовинску или неимовинску) или да другоме нанесе какву штету.

ПОСЛЕДИЦЕ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА

- Штете настале вршењем компјутерских деликата, зависно од појавног обилика компјутерског криминалитета, могу се поделити на:
  - финансијске – које могу да настану када учинилац врши дело у циљу стицања противправне имовинске користи, па ту користи за себе или друго, заиста и стекне, или је не стекне, али својим делом објективно причини одређену штету, или када учинилац не поступа ради стицања користи за себе или другог, али објективно учини финансијску штету.
  - нематеријалне – које се огледају у неовлашћеном откривању туђих тајни, или другом "индискретном штетном поступању"
  - комбиноване – када се откривањем одређене тајне, или повредом ауторског права, путем злоупотребе компјутера илиинформатичке мреже наруши нечији углед, односно повреди морално право а истовремено проузрокује и конкретна финансијска штета.

Високотехнолошки криминалитет може да произведе далеко теже последице по приватни и јавни интерес, јер географска раздаљина и државне границе не представљају препреку за извршење кривичног дела.

СУПРОТСТАВЉАЊЕ ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛИТЕТУ

- Борба против компјутерског криминала заснива се на превентивним и репресивним мерама.
- Репресивне оперативно-тактичке мере су исте као и код других видова криминалитета.
- Превентивне мере су специфичне. Оне су усмерене на предузимање активности у циљу отклањања извора. услова, околности или пропуста који погодују неовлашћеном коришћењу или злоупотреби компјутера.
- Превентивним мерама треба обезбедити:
  - а) идентифнкацију могућих напада на компјутер и њихову класификацију с аспекта вероватноће реализације, објекта напада, начина и последица реализације;
  - б) избор и постављање одговарајућег механизма заштите;
  - в) одржавање, проверу и унапређење постављеног механизма заштите.

ПРЕВЕНЦИЈА – НАЈСИГУРНИЈИ ОБЛИК ЗАШТИТЕ

Савети грађанима:

- Увек држати укључен заштитни програм на рачунару и ажурирати га
- Ажурирати оперативни систем
- Угасити рачунар када нисте у кући
- Не одговарати на спам поруке, уколико нисте сигурни да познајете пошиљаоца
- Избегавати коришћење личних података на Интернету
- Лозинке за електронске налоге никада не би требало чувати аутоматски у пољима за унос
- Избегавати остављање фотографија на Интернету, нарочито деце, које могу бити јавно доступне свим корисницима

Савети за родитеље:

- Ако сазнате да је дете било изложено насиљу путем Интернета, потребно је:
- научити дете да не одговара на насилне, претеће или било које друге сумњиве поруке и позиве;
- не бришите поруке или слике јер могу послужити као доказ;
- контактирајте са Интернетом провајдера и пријавите да сте примили такву поруку;
- обавестите школу о понашању – злостављању или евентуалним променама расположења и понашања код детета;
- обавестите полицију ако поруке садрже претње насиљем, ухођење, напастовање, дечију порнографију, или када претходни кораци нису дали резултате;
- ако Вам је познат идентитет извршиоца, број или електронска адреса са које су узнемирујуће и злонамерне поруке упућене, свакако обавестите о томе полицију, мобилне оператере, Интернет провајдера, школу...

ПРОБЛЕМИ ДОКАЗИВЊА

- специфични трагови који се огледају у променама у сфери електронских записа које су настале у софтверском делу рачунара
- анонимност криминалаца и тешко установљавање трагова које иза себе оставља неовлашћено продирање у туђе компјутерске системе
- IP адреса није увек поуздано средство за праћење путање кретања лица које је упало у компјутерски систем зато што и њоме може да се манипулише
- откривање, тумачење и доказно коришћење промена насталих у софтверу захтева изузетну стручност и ангажовање компјутерских експерата високог нивоа којих данас има веома мало
- различито место и време деловања и извршења кривичних дела компјутерског криминалитета

- Дискусија
- Питања

- Хвала на пажњи