ИНТЕРВЈУ

МАРЈАН РИСТЕСКИ, ИНСПЕКТОР ЗА КОМПЈУТЕРСКИ КРИМИНАЛ

Во Македонија првиот случај е забележан во 1997 година и до денеска се откриени 21 дело и 27 сторители.

Овој вид на криминал се шири со голема динамика и со богатство од појавни облици, бидејќи станува збор за технологии со големи можности и примени во секојдневниот живот.

Пронаоѓањето на докази во вакви случаи се врши преку "електронските траги" кои се обезбедуваат со вештачења на компјутерите.

БОРБА ПРОТИВ С

Разговорот го водеше:
Рената МАТЕСКА

Господине Ристески, во последно време многу е актуелно вршењето на кривично дело со помош или посредство на компјутер. Што МВР презема на овој план?

РИСТЕСКИ: Компјутерот претставува една од најзначајните и најреволуционерни откритија во развојот на техничко-технолошката цивилизација. Информатиката како млада наука се развива со побрзо темпо од која било друга наука на планетава. За само 50-тина години се откриени и усовршени многу уреди за складирање и обработка на огромни количини на податоци. На други науки им требало цели епохи за да достигнат такво ниво на знаења и искуства. Но, и покрај сите предности и корист кои компјутерот со себе му ги носи на човештвото, компјутерот за жал брзо стана и средство на злоупотреба на несовесни поединци, групи или дури и на организации. Една понова американска студија од оваа област укажа на фактот дека овој вид на криминалитет се случува дури 40 пати почесто од класичниот криминалитет, а дури 90 отсто од информатичките кривични дела остануваат практично неоткриени, односно во темната бројка на криминалитетот, бидејќи откривањето и докажувањето кај овој вид криминал е исклучително тешко. Овој вид на криминал се шири со голема динамика и со богатство од појавни облици, бидејќи станува збор за технологии со големи можности и примени во секојдневниот живот. Криминалците кои вршат и класични кривични дела ја сфатија моќта и предностите на компјутерите, па така често пати ги употребуваат како помошно средство и при вршење на класични кривични дела.

Во овој контекст МВР преку своите експерти кои работат на оваа проблематика ги следи новите светски трендови на откривање и санкционирање на најмодерниот криминал на денешнината и при секое сознание дека е извршено кривично дело од областа на компјутерскиот криминал вршејќи ја својата законска обврска, веднаш презема мерки за откривање на делото-а и сторителот-те. Најчесто пронаоѓањето на докази во вакви случаи се врши преку "електронските траги" кои се обезбедуваат со вештачења на компјутерите со кои се вршеле овие кривичните дела и потоа се поднесува кривична пријава по член 251 од Кривичниот законик против сторителите.

Може ли накусо да ги запознаеме читателите со историјатот на компјутерскиот криминал во светот и во Република Македонија?

РИСТЕСКИ: Компјутерскиот криминал се појавува за прв пат при крајот на 60-те, а се интензивира во почетокот на 80-те години со појавата на PC персоналниот компјутер и со појавата на првите BBS мрежни системи. Првите компјутери биле сместени во огромни простории со специјални климатски услови и само одредени лица имале пристап до нив. Програмерите кои работеле на овие компјутери користеле одредени рутини кои ги викале со заедничко име "hacks" за да си ја олеснат работата, па подоцна од овој термин и настанува зборот хакер. Со појавата на првиот IBM PC персонален компјутер, овие пред тоа стриктно професионални машини почнуваат да се користат насекаде, па подоцна се

АЈБЕР-КРИМИНАЛЦИТЕ

појавува и потребата од нивно вмрежување поради полесна размена на податоците и така се појавуваат првите приватни BBS системи на кои хакерите си разменуваат идеи и искуства. Со појавата на Интернет како глобална планетарна мрежа кој од ден на ден се шири сè повеќе, хакерите веќе имаат можност да ги надминат ограничувањата на државните граници и континенти и делуваат на планетарно ниво при вршењето на овие кривични дела.

Во Македонија првиот случај е забележан во 1997 година и до денеска се откриени 21 дело и 27 сторители. Во поглед на начините на извршување на овие дела кај нас во минатото може да се каже дека често одредени сторители со неовластено навлегување во компјутерските системи на интернет провајдерите бесплатно користеле интернет услуги посебно кога овие услуги беа скапи пред неколку години. Исто така, има случаи на неовластено навлегување во компјутерските системи на македонски телекомуникации за бесплатно користење на телефонски услуги од страна на сторителите, преку неоригинални чип картички со импулси посебно приготвени неограничено да траат. МВР има поднесено и неколку пријави против одговорни службени лица во банкарски институции и приватни фирми кои злоупотребувајќи ја својата службена положба имаат избришано податоци или внесено лажни податоци во компјутерите на тие институции поради стекнување на имотна корист за себе или за нивни блиски лица.

Покарактеристичен беше најновиот случај од 2003 година кога во Комерцијална и Стопанска банка имаше неовластено навлегување во компјутерските системи преку користење на лажни кредитни картички од типот VISA, MASTERCARD и други при подигање на готовина од банкомати и на овој начин сторителите имаа противправно стекнато значителна имотна корист.

Кои се најпознатите светски хакери кои веќе, така да кажеме, останаа забележани во историјата на хакерството?

РИСТЕСКИ: Ќе ги наведам по редослед. На прво место е Кевин Митник, алијас Кондор. Легендата на хакерството во светот е секако Митник и претставува културен херој на сајбер-спејсот и инспирација за новите хакери кои го учат занаетот. Првото обвинение против него е покренато уште во 1995 година поради фалсификување на 20.000 броеви на кредитни картички, неовластено навлегување во системите на компаниите Моторола, Сун Микросистемс, Нокиа Фујитсу и многу други и предизвикување на штета која е проценета на 80 милиони долари. Честопати навлегувал и во системите на државните институции на САД како системот на северноамериканската команда за одбрана НОРАД уште во 1983 година НАСА, па дури и на ФБИ кој и го апси во 1992 година. Последната затворска казна му беше пет години и забрана за пристап на интернет со 21 јануари 2003 година. Долго време беше помеѓу 10 најбарани криминалци на сајтот на ФБИ. Инспирација е за неколку холивудски филма како "Воени игри", "Takedoun" и други.

Втор најпознат хакер е Владимир Левин, Русин по потекло од Петроград кој успеал да навлезе во системот на Citybank во САД во 1994 година и да извлече 10 милиони долари. Ова е неговиот најголем потфат, но е откриен и уапсен, а Citybank успева да го поврати најголемиот дел од сумата.

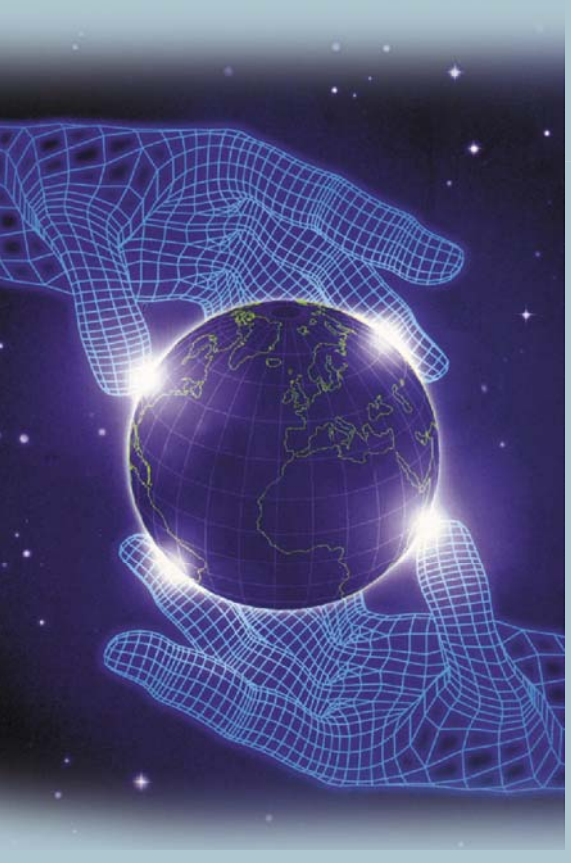
Кои се појавните облици и начини на извршување на кривични дела од областа на компјутерскиот криминал?

РИСТЕСКИ: Облиците и начините се - компјутерска измама, финансиски кражби и злоупотреби, фалсификување на податоци и документи, компјутерски вандализам, изработка и употреба на компјутерски вируси, компјутерска саботажа и шпионажа и хакерство. Кај компјутерска измама се работи за кривично дело кога одредено лице ќе внесе одредени неточни податоци или нема да внесе одреден важен податок со цел тоа да влијае на резултат на електронската обработка или преносот на податоците и така за себе или за друг противправно да прибави одредена имотна корист или да нанесе штета на друг. Финансиските кражби и злоупотреби со помош на компјутер се едни од најчестите компјутерски криминални дела и се однесуваат на злоупотреба на кредитни картички кои пак се едни од најмодерните платежни средства, и на разни навлегувања во заштитени системи и правење на недозволени финансиски трансакции. Сегашниот степен на развој на компјутерите дозволува дигитализација и менување на содржината на разни акти и документи кои се користат при правниот сообраќај, како и на фалсификување на податоци кои се во електронска форма. Дури честопати постојат и обиди за фалсификување на банкноти со помош на компјутер и периферни уреди како скенер, печатар чие усовршување денес е на високо ниво дури и кај уредите за широка потрошувачка. Под компјутерски вандализам се подразбира намерно навлегување во туѓи компјутери и заштитени компјутерски системи и

ИНТЕРВЈУ

МАРЈАН РИСТЕСКИ, ИНСПЕКТОР ЗА КОМПЈУТЕРСКИ КРИМИНАЛ

бришење и уништување на податоци без некоја посебна цел, туку само да се предизвика одредена штета кај системите кои се објект на напад во поглед на нивно правилно функционирање. Софтверот односно програмите се едно од најмоќните оружја на сајбер-криминалците. Под поимот компјутерски вируси се мисли на програми кои несовесни поединци ги пишуваат за да нанесат што поголема штета на многу компјутери врзани во мрежа како на пример на глобалната Интернет-мрежа. Нивни основни одлики се: се копираат самите себеси на секој компјутер со кој ќе дојдат во контакт. Не се забележливи, односно најчесто се невидливи за корисникот на компјутерот, посебно ако на компјутерот не е инсталиран специјализиран софтвер за нивна детекција. Автоматски извршуваат одредени команди како бришење на корисни податоци на компјутерот на жртвата, или пак ги испраќаат податоците на одредена друга локација на мрежата без знаење на сопственикот на компјутерот. Покрај хакерите и групите што тие ги организираат за неовластено навлегување во заштитени системи, на денешно време постојат и специјализирани тајни владини служби кои преку навлегување во компјутерскиот систем на другите држави прибавуваат податоци од разузнавачка природа. Така под поимот компјутерска шпионажа може да се дефинира еден од најмодерните облици на разузнавање, но исто така постои и индустриска шпионажа која е само од комерцијална природа. Компјутерска саботажа имаме во случај кога некој ќе уништи, избрише, промени, прикрие или на друг начин ќе онеспособи податок, програма или ќе го оштети компјутерот кој е од значење за државен орган, институција, јавна служба. Сајбер-криминалците или популарно наречени хакери се по правило лица со посебни стручни и практични знаења и вештини од доменот на високата информатичка технологија кои своите



РЕПУБЛИКА МАКЕДОНИЈА
МИНИСТЕРСТВО ЗА ЕКОНОМИЈА

ИЗВЕСТУВАЊЕ

Владата на Република Македонија донесе одлука за реализација на проект за засилување на капацитетот на дипломатско – конзуларните претставништва (ДКП) на Република Македонија со економски претставници.

Во 2004 година, се планира испраќање на следните економски претставници:

- економски советник за трговска промоција во ДКП во Србија и Црна Гора
- економски советник за трговска промоција во ДКП во Русија
- економски советник за инвестициона промоција во ДКП во Германија
- економски советник за инвестициона промоција во ДКП во Италија

Економските советници ги предлага министерот за економија, а во ДКП ги упатува министерот за надворешни работи, при што имаат ист статус како и сите вработени во дипломатско – конзуларните претставништва.
Кандидатите за економски советници ќе поминат кус ефективен период на обука во Министерството за надворешни работи.

Министерството за економија ги повикува сите лица заинтересирани за работа како економски советници во некое од наведените ДКП-а, да достават писмо за интерес и професионална биографија до Министерството за економија. Заинтересираните лица особено треба да ги исполнуваат следните услови:

- Високо образование;
- Одлично познавање на јазикот (пишување и говорење) на земјата за која искажува интерес;
- Познавање на друг светски јазик би била предност;
- Најмалку три години непрекинат престој во земјата за која искажува интерес во последните десет години;
- Соодветно работно искуство и референци;
- Да се државјани на Република Македонија со место на живеење во земјата или во странство.

Заинтересираните лица што ги исполнуваат бараните услови, можат да бидат земени предвид за поширок избор на кандидати за економски советници, согласно законските прописи и процедури за вработување државни службеници и упатување лица во дипломатско – конзуларните претставништва на Република Македонија.

Писмата со интерес, заедно со придружната документација треба да се достават на адреса на Министерството за економија: "Јуриј Гагарин" број 15, 1000 Скопје, најдоцна до 15 февруари 2004.

знаења ги користат за нанесување на штети на одредени заштитени системи. Хакерството како модерен феномен произлегува од техничкиот предизвик да се пробие заштитата на одреден информатички систем и да се навлезе во него. Колку е заштитата посилна, толку е предизвикот поголем. Овие кривични дела се вршат прикриено без просторна поврзаност помеѓу сторителот и жртвата и по правило тешко се докажуваат и остануваат во темната бројка на криминалитетот. Честопати дури ни администраторите на мрежните системи не можат да забележат неовластено навлегување во системот од страна на хакер сè додека системот не претрпи некоја штета.

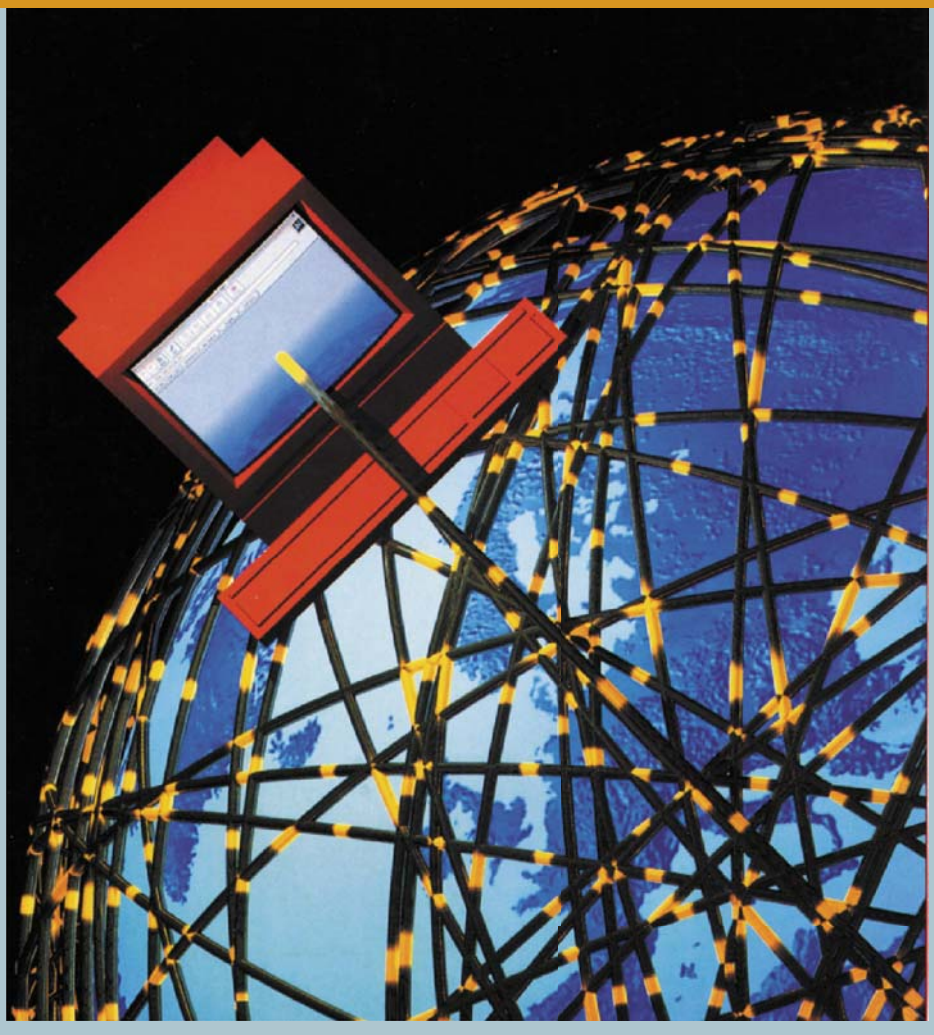
Постојат ли начини на дознавање, мерки за откривање на сторителите и докажување на компјутерскиот криминал?

РИСТЕСКИ: Редоследно постапката е следна: пријава од оштетен, откривање од страна на администраторите на информатичките системи, истрагата и докажувањето мора да го прават стручни лица со посебни, стручни и практични знаења и компјутерска форензика. Еден од најчестите начини за дознавање на кое било кривично дело, па така и на кривични дела од областа на компјутерскиот криминал, е секако пријавата од оштетениот. Во оваа смисла под поимот оштетен можат да бидат физички и правни лица, државни органи и институции. На пример, кога стручните лица кои ги одржуваат и администрираат информатичките системи ќе забележат дека дошло до неовластено навлегување во системот кој тие го одржуваат однадвор и дека настанала одредена штета во смисла на губење на податоци или на целокупното работење на системот, секако дека ова неовластено навлегување треба да го пријават до соодветен државен орган кој е надлежен понатаму да постапи, со цел пронаоѓање и санкционирање на сторителот. Стручните овластени лица на овој орган ќе го проценат видот и обемот на настанатата штета и ќе преземат понатамошни мерки. Истражувачите на овој вид криминал понекогаш користат оригиналнса апликациска програма, а понекогаш специјален софтвер за анализа и алатки за истражување. Истражувачите најдоа начини за собирање траги од оддалечен компјутер до кој тие немаат непосреден физички пристап, спроведувајќи пристап преку телефонска линија или мрежна конекција. Дури е можно да се следат активностите на компјутерска мрежа преку интернет. Овие процедури формираат дел од она што е наречено компјутерска форензика, па некои луѓе исто така го користат овој термин при употреба на компјутерот за анализа на комплексни податоци (на пример конекции помеѓу индивидуи со испитување на телефонско логирање или трансакции преку банки). Другата употреба на терминот е кога компјутерите се искористени во судот во форма на компјутерска графика за да илустрираат комплексна ситуација, или како замена на голем волумен на листови - базирани на истражувања и состојби. Што е всушност компјутерска форензика? Компјутерска форензика е доказ од компјутер кој треба да биде издржан, убедлив и доволен за судот да може да го прифати. Во форензичко-информатички постапки без разлика колку и да се внимателни луѓето кои имаат за цел да крадат електронски информации тие оставаат траги од нивните активности. Исто кога сторителите се обидуваат да го уништат доказот кој е на компјутер тие позади себе оставаат траги. Во двата случаи може да се докаже дека овие траги може да се пронајдат и да се презентираат пред судот. Компјутерските форензички специјалисти прават повеќе од вклучување на компјутерот и листање на фолдери и пребарување на фајлови. Тие треба да бидат способни да извршат комплексни "evidence recovery procedures" со вештина и експертиза која ќе го држи кредибилитетот на електронските докази пред судот. Во основа овие постапки опфаќаат: копирање на податоци, барање на докази од електронска пошта и друга интернет комуникација, враќање на податоци, пребарување на документи и други податоци.

Каква е законската регулатива кај нас и во светот за компјутерскиот криминал?

РИСТЕСКИ: Кај нас санкционирањето на овие кривични дела е регулирано со член 251 од Кривичниот законик, член 251 од КЗ на (навлегување во компјутерски систем) службен весник бр. 37/1996 година.

Кај нас ова кривично дело е внесено во КЗ во 1996 година и од тогаш па наваму се применува овој член во практика. Спаѓа во глава 23, Кри-



вични дела против имотот од КЗ на Р. Македонија. Став 1 од овој член вели: Тој којшто неовластено ќе внесе измени, објави, скрие, избрише или уништи компјутерски податоци или програми, или на друг начин ќе навлезе во компјутерски систем со намера за себе или за друг да прибави противправна имотна корист или да оштети друг - ќе се казни со парична казна или со затвор до три години.

Во Германија тоа е регулирано со Закон за сузбивање на стопански криминал од 1986, Компјутерска шпионажа член 202 а; компјутерска измама чл. 263 а; Промена на податоци чл. 302 а; компјутерска саботажа чл.303 а. Во Австрија регулирано е во1989, чл. 126 а. оштетување на податоци. Англија во 1990 со Закон за злоупотреба на компјутери кој предвидува повеќе кривични дела ја регулира оваа проблематика. Во Република Словенија - Казнен закон 1999 чл. 225 Противзаконски влез во заштитена база на податоци; чл. 242 - Навлегување во компјутерски систем, додека во Република Хрватска компјутерскиот криминал е регулиран во 1996 година со член 223 - Оштетување и употреба на туѓи податоци.

Постои ли превенција за компјутерскиот криминал?

РИСТЕСКИ: Мерки кои треба превентивно да се преземат против компјутерскиот криминал најчесто се: информатичка едукација, администрирање на информатичките системи од стручни лица, користење на заштита од неовластени навлегувања (хардверски и софтверски сигурносни системи) и санкционирање на овие кривични дела.

Под информатичка едукација овде се мисли на едукација на секој поединец којшто користи компјутер да му се укаже на опасностите од компјутерскиот криминал, посебно на младата генерација којашто е и најголем корисник на информатичката технологија. Со оваа едукација секој поединец ќе знае како да се заштити од сајбер-натрапниците или од компјутерските вируси пред да настанат штетните последици. При избор на администратори кои се грижат за сигурноста на информатичките системи, треба да се внимава на нивното соодветно образование и искуство за тие да бидат чекор понапред со знаењата од компјутерските криминалци и да применат соодветно пропишано ниво на заштита (хардверско и софтверско) на системите кои ги администрираат.

При изборот на сигурносни системи треба да се користат современи проверени технологии од оваа област за да се минимизира ризикот од оставање на т.н. сигурносни дупки во системот кои хакерите вешто ги користат за да навлезат во системот. Секако имајќи го предвид нивото на општествената опасност од овој вид на криминал државата треба да пропише соодветни санкции за сторителите на овие кривични дела кои ќе послужат како сериозна закана врз многу поедници кои нема да го прифатат техничкиот предизвик на навлегуваат во заштитени системи и да стекнуваат имотна корист на овој начин.

Можеме ли да констатираме дека компјутерскиот криминал е голема општествена опасност и што се треба да направиме за да го спречиме?

РИСТЕСКИ: Овој вид криминал лесно ги надминува границите на државите и има интернационален карактер и висината на штетата која настанува со вршењето на овие кривични дела од ден на ден е сè поголема. Дури и меѓународните терористички организации сè повеќе ги користат компјутерите и глобалната мрежа за остварување на своите цели. Секоја современа држава треба да преземе навремени соодветни мерки за превенција и санкционирање на овој вид криминал. Бидејќи овој вид криминал не знае за просторни граници, оформувањето на специјални тимови во рамките на Интерпол кој се занимаваат со истражување на овие кривични дела ќе има голем придонес во успешноста на справувањето со најмодерниот вид на криминал во сегашноста и иднината. Секој поединец кој користи компјутер приватно или професионално треба да биде свесен за опасноста и да користи специјализиран оргинален софтвер за заштита од компјутерски напади и компјутерски вируси со што би ги минимизирале шансите на сајбер-криминалците да предизвикаат штета. Исто така, сторителите на овие дела покрај санкционирањето треба да се ресоцијализираат преку нивно вклучување во позитивните страни на информатиката, за да се искористат нивните знаења кои дотогаш ги користеле за деструктивни дејства.