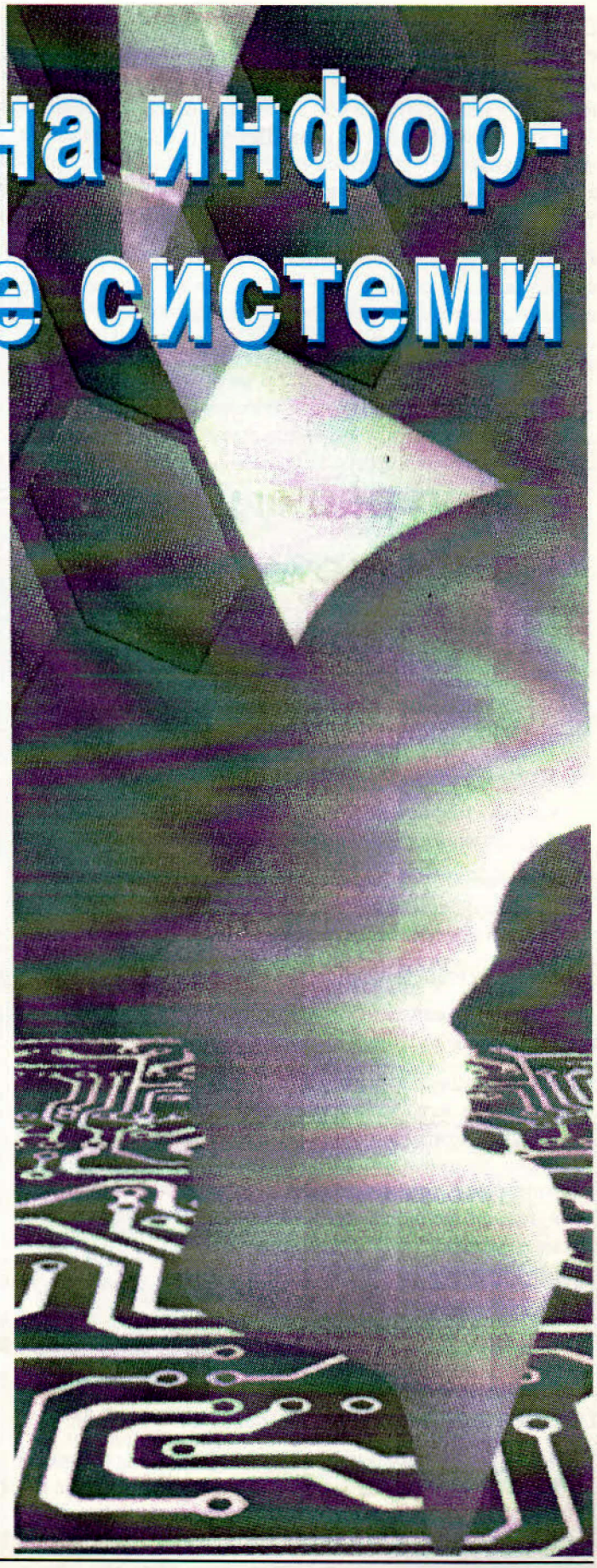
Заштита на информационите системи



Томе Димитриевски,
ИСМ - Информациски Системи и Менаџмент

Самиот термин заштита на информациони системи се толкува на различни начини. Многу често тој се поистоветува со криптирањето на податоци и контрола на пристапот во просторот каде е сместена компјутерската и комуникациона опрема. Исто така неправилно се преведуваат и користат странските изрази security, protection, privacy кои често се среќаваат во информатичката термиинологија, како и зборовите firewall, trojan hors, virus, logic time bomb, worm. Некои корисници сметаат дека заштитата е работа само на државата (да ги заштити своите витални информации најчесто поврзани со безбедноста и одбраната) или дека тоа е работа на специјалисти кои едноставно ќе ги ангажираат да го решат проблемот кога ќе се случи и ако се случи.

Можеби и зборот заштита не е најсоодветен за оваа намена и затоа сметам дека на самиот почеток треба прецизно да се дефинира што се подразбира под заштита на информационите системи.

Заштитата на информационите системи е комплексна активност која ја спроведуваат сите, кои на било кој начин се поврзани со него, било само како корисници или задолжени за неговото функционирање. Заштитата опфаќа мерки и постапки, дефинирани и разработени во процедури со цел да овозможи информациониот систем да ги извршува целите за кои е проектиран. Сервисите кои ги овозможува треба да се расположиви во секое време, информациите да се точни и достапни и тоа само на оние за кои се наменети. Информациониот систем треба да е доволно жилав и надежен за да може да ги извршува задачите за кои е проектиран и во неповолни услови и да може доволно брзо да се опорави доколку сепак дојде до прекин во неговото работење.

Затоа имателот на информациониот систем пред се треба да изгради јасна политика која треба доследно да се спроведува за да се обезбедат бараните цели.

Прво треба да се изврши проценка на вредноста инвестирана во просторот и опремувањето, како и вредноста на информациите. Следна активност е идентификација и процена на ризиците на кои е изложен информациониот систем. Откако овие работи ќе бидат завршени се пристапува кон изработка на студија од која ќе произлезе политиката на имателот на информациониот систем.

Проценката на материјалната вредност е релативно едноставна за разлика од проценката на вредноста на информациите. За тоа постојат методи кои воглаввно ги класифицираат информациите на:

- ***корисни*** - информации кои се потребни во секојдневното работење, но кои истовремено можат да се обезбедат и од други извори и кои не се значајни за донесување на одлуки (вредност помала од 10.000 долари)
- ***вредни*** - информации значајни за деловното работење и донесување на одлуки (вредност до 1.000.000 долари) и
- ***критични*** - информации од трајна вредност, без кои не е можно продолжување на работата и кои, ако му се расположиви на непријателот или конкуренцијата ќе предизвика штета поголема од 1.000.000 долари.

Истовремено информациите се класифицираат како:

- ***јавни*** - информации кои се достапни до сите субјекти под еднакви услови и чиј извор е надворешен
- ***приватни*** - информации поврзани со деловното работење од кои дел е расположив и за субјекти од надвор, но воглавном се деловна тајна
- ***лични*** - информации поврзани со конкретна личност

На овој начин се утврдува вредноста и значењето на информациите.

Идентификацијата на ризиците и веројатноста на нивно појавување е исто така сложен процес. Во секој случај треба сите идентификувани ризици да се третираат иако за некои од нив нема да се применат мерки за нивно елеминирање или намалување на штетните влијаниа, дали заради високата цена или затоа што не постојат такви мерки.

Основна класификација на ризиците е спрама местото на појавување и тоа:

- ***надворешни*** - на кои не можеме да влијаеме и
- ***внатрешни*** - предизвикани од самите вработени.

По природата на појавување се делат на:

- ***природни*** - природни катастрофи (поплава, земјотрес, ...)
- ***предизвикани од човек*** - намерни или ненамерни без оглед на целта
- ***оперативни*** - техничка неисправност на машинската и програмската опрема на информациониот систем, како и пратечката опрема (климатизација, напојување со електрична енергија, ...)

За да може да се изврши правилен избор на мерките за заштита, секако дека треба да се познаваат и целите и мотивите за деструктивното однесување на поединци или организации, а тие са:

- ***Да се здобие со материјална корист*** за себе или за организацијата (промена на состојбата на сметките кај банките, тарифирањето на телефонските импулси, продавање на информации на конкурентски фирми или држави).
- ***Да ги искористи за политички цели*** (се интензивираат за време на избори).
- ***Да ја намали конкурентноста на претпријатието***.
- ***За воени цели*** (да се онеспособат непријателските системи за набљудување и наведување).

Студијата која следи по завршувањето со претходните активности треба детално да ги обработи добиените податоци, да определи конкретни мерки кои ќе се применуваат, да ја определи организацијата и носителите на секоја активност, да ги дефинира прецизно одговорностите, да ги разработи процедурите, да ја дефинира контролата и на крај цената.

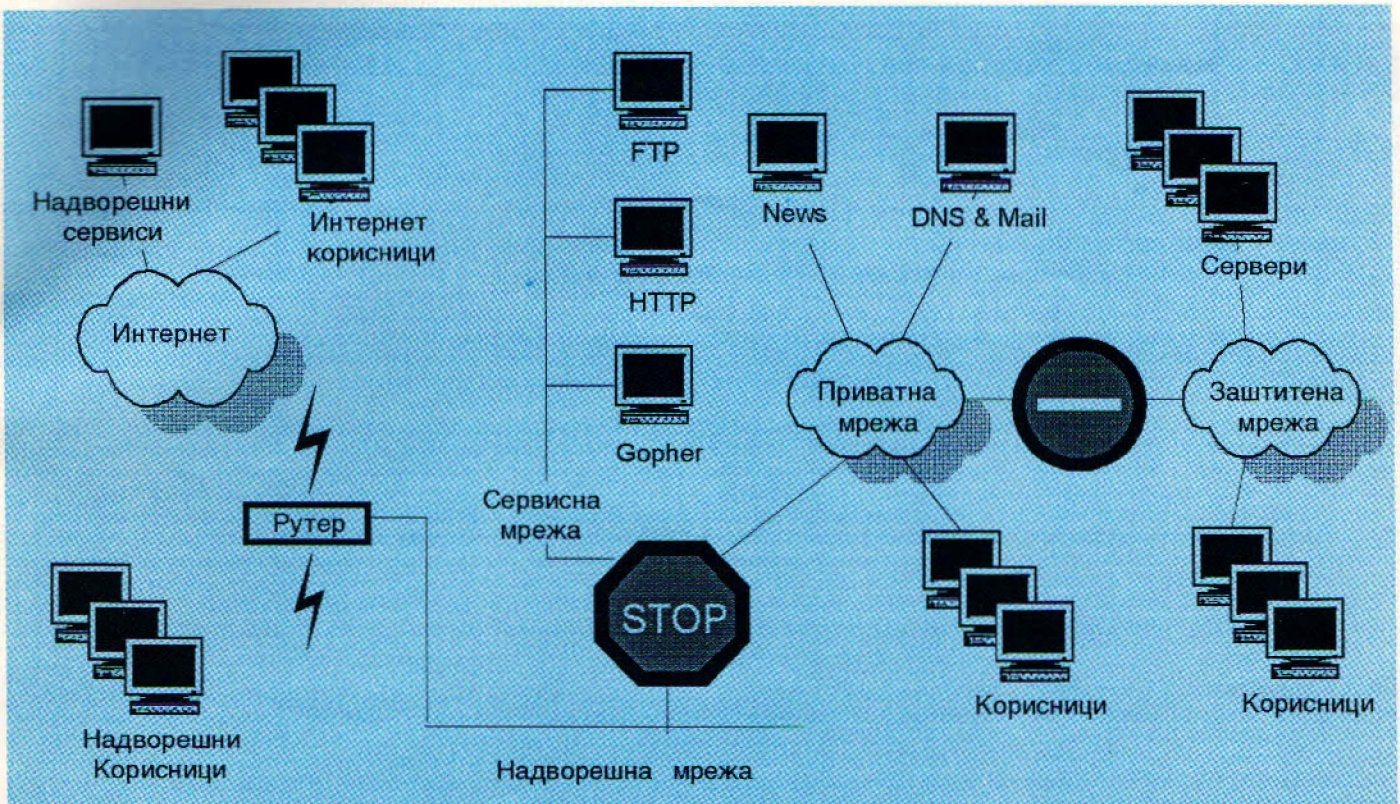
Многу значајна е улогата на врвното раководство во целиот овој процес и затоа треба уште од самиот почеток нивно ангажирање за да може изградената политика и во пракса да се применува.

Перманентното пратење и усовршување е исто така многу значајно.

Едукацијата на кадрите е еден од најважните сегменти во спроведувањето на заштитата и тоа не само на оние непосредно задолжени за функционирањето на информационите системи, туку и на нивните корисници.

Министерството за наука, во текот на 1996 година организира два семинари. Воведниот дводневен семинар „Стратегија на заштитата на информационите системи " се одржа на 30 и 31 мај, 1996 година во Скопје. Предавач на семинарот беше дипл. инж. Вања Жиберна, експерт во областа на заштитата на информациони системи, кој повеќе од дваесет години е присутен на просторите на поранешна Југославија и пошироко, учесник во повеќе проекти во оваа област, а сега е вработен како „Security officer" во Словенија. На овој семинар присуствуваа повеќе од 50 слушатели, раководители на информациони центри на органите на државната управа и јавните претпријатија.

Семинарот „Information systems security workshop" се одржа во Охрид од 21 до 24 октомври, 1996 година. На овој семинар учествуваа повеќе од дваесет слушатели од органите



Хипотетичен модел на современ информационен систем

на државната управа и јавните претпријатија. Предавач на семинарот беше Mr. Robert J. Wilk, магистер на Политехничкиот факултет во Њујорк, претседател и основач на IACSS - International Association for Computer Security Inc., „гуру" во оваа област кој одржал повеќе од 200 семинари во целиот свет и е автор на десетина книги од оваа област.

Следни активности, кои Министерството за наука веќе ги превзема:

- набавка на современи софтверски и хардверски решенија и нивна имплементација;
- организирање на специјализирани семинари;
- пратење на светските достигнувања и

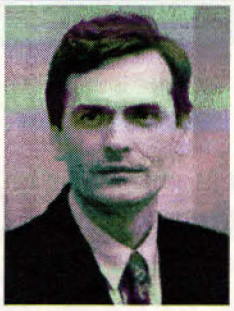
нормативно уредување на оваа проблематика, компатибилно со светот.

Не постои апсолутна, ниту едноставна заштита на информационите системи. Таа треба перманентно да се развива и што е најважно сите ние да бидеме свесни дека цената што треба да ја платиме е многу помала од вредноста на информациониот систем.

На крајот предлагам да го погледате моделот на современ информационен систем на сликата, од кој јасно се гледа целата негова комплексност и сложеност. Ваков систем не би можел да функционира и да ги остварува целите кои од него се очекуваат без да се заштити во сите негови сегменти.

На сликата е прикажан хипотетичен модел на современ информационен систем, кој што често се применува во развиениот свет, а во последно врема станува присутен и кај нас.

На моделот јасно се разграничени две целини: внатрешна и надворешна мрежа. Внатрешната мрежа содржи подмрежа (заштитена) со витални податоци за системот. Критичните места во мрежата (означени со сообраќајни знаци) ги означуваат правилата на комуницирање во системот.



Томе Димитриевски е роден 1955 година во Битола. Електротехнички факултет завршил во Скопје,1980 год. Досега работел во: Искра - телематика, Министерство за внатрешни работи и Министерство за народна одбрана, а сега работи во ИСМ - Информациски Системи и Менаџмент ДОО - Скопје, како управител на друштвото. Член е на Комисијата за изработка на стандарди за единици за внесување на податоци и множества на знаци, кодирање и системи за шифрирање при Заводот за стандардизација и метрологија. Учествувал во повеќе проекти од областа на заштита на информационите системи на просторот на поранешна Југославија.