Насоки за нивоа на доверливост на информациите и нивоа на пристап до нив

Нивоата на заштита од неовластен пристап до информациите во информациските системи на органите се следните:

- ниво "0" или "D" - ниво на слободен пристап;
- ниво "1" или "C" - ниво на слободно управување на пристап;
- ниво "2" или "B" - ниво на принудно управување на пристап;
- ниво "3" или "A" - ниво на голема безбедност.

Основните мерки на заштита кои треба да се применат при секое од овие нивоа се следните:

1. Ниво "0" или "D" опфаќа јавни и општо достапни информации (на пример објавувани на веб-локациите на органите). Тогаш е предвидено анонимно користење на информацијата и не е потребно користење на механизми со кои се постигнува доверливост на информацијата.

2. Ниво "1" или "C" бара примена на следните основни мерки:
а) корисниците да се идентификуваат, пред да можат да преземат било каква акција – автентикација;
б) за докажување на идентитетот треба да се користи заштитен механизам од типот корисничко име/лозинка. Не се потребни дополнителни проверки за основните податоци на корисникот;
в) пристапот до точно определени информации да биде пропишан на точно определени корисници – авторизација;
г) потребно е воспоставување на доверлива комуникација помеѓу корисниците и системот со користење на криптографски протоколи;
д) информациите од точка б) кои се користат за докажување на идентитетот на корисниците кои пристапуваат во системот треба да бидат заштитени од неовластен пристап;
ѓ) системот за контрола на пристап треба да функционира самостојно, заштитен од надворешни влијанија и од обиди да се следи текот на неговата работата;
е) информацискиот систем треба да располага со технички и/или програмски средства, со кои ќе може периодично да се проверува валидноста на системот за контрола на пристап.
ж) заштитните механизми треба да имаат поминато тест, којшто ќе потврди дека корисникот нема можност да ги заобиколи и да добие неовластен пристап до информациите кои тие ги штитат.

3. Ниво "2" или "B" бара примена на основните мерки набројани во претходното ниво и дополнително примена на следниве мерки:
а) како механизам за проверка на идентитетот на корисниците да се користи електронски потпис, независно дали е издаден за употреба во локалната инфраструктура на јавен клуч во рамките на конкретниот орган, или е издаден од надворешен доставувач на доверливи услуги;
б) при издавање на електронски потпис органот дополнително ги проверува основните податоци за корисникот, без да е потребно негово лично присуство;
в) потребно е воспоставување на доверлива комуникација помеѓу корисниците и системот преку протоколот SSL (Secure Sockets Layer), протоколот TLS (Transport Layer Security) или VPN (Virtual Private Networking) решение.
г) доверливиот информациски систем треба да обезбеди реализација на принудно управување на пристапот до сите објекти, според претходно строго дефинирани правила на пристап;
д) доверливиот информациски систем треба да обезбеди взаемна изолација на процесите преку разделување на адресниот простор.

4. Ниво "3" или "A" бара примена на мерките набројани во двете претходни нивоа и дополнително примена на следниве мерки:
а) како механизам за идентификација да се користи електронски потпис издаден од владина инфраструктура на јавен клуч;
б) при издавање на електронскиот потпис од ставот 4 алинеа 1, потребна е физичка потврда за идентитет на лицето;
в) потребно е воспоставување на доверлива комуникација помеѓу корисниците и системот согласно следниве препораки:

- За остварување на заштитена размена на пораки по протоколите HTTP, LDAP, FTP и други, да се користи протокол TLS (Transport Layer Security) или VPN (Virtual Private Networking) решенија за безбедносно криптирање на сесиите.
- За криптирање на XML базирани пораки на ниво на сесија да се користи протоколот XMLENC.

Потребни се и соодветни мерки за криптирање на информациите при нивното чување. Минималната должина на симетричен клуч треба да биде 128 бита.
Ваквите решенија пред имплементација треба да бидат ревидирани од овластено тело утврдено со закон.
г) доверливиот информациски систем не смее да дозволи намалување на неговата безбедност како резултат на долготрајни обиди за нејзино нарушување;
д) доверливиот информациски систем треба да има механизми за регистрација на обидите за нарушување на неговата безбедност.