ИНФОРМАЦИОНА БЕЗБЕДНОСТ У СИСТЕМУ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Информациона безбедност тајних података обухвата интегрисани скуп међузависних мера и активности усмерених на заштиту тајних података које се обрађују у ИКТ системима (ИКТ- информационо комуникационе технологије). Процесом безбедносне акредитације ИКТ система утврђује се да ли је систем постигао адекватан ниво заштите тајних података.

Безбедносна верификација ИКТ система обезбеђује:

- потврду да ли су планиране мере безбедности ИКТ система правилно спроведене;
- потврду да је одговарајућим тестирањем постигнут захтевани ниво безбедности;
- документовање резултата верификације безбедносне имплементације ИКТ система;

Ово потврђује да су испоштовани минимални безбедносни стандарди ИКТ система за обраду, чување и размену тајних података.

Проценом могућег нарушавања безбедности тајних података и безбедности ИКТ система, односно проценом безбедносног ризика, утврђује се вероватноћа да ће одређена рањивост тог система бити искоришћена и довести до нарушавања безбедности система.

Процена безбедносног ризика служи за утврђивање безбедносних ризика, тј. претњи и рањивости ИКТ система, утврђивање њихове величине, како би се идентификовале области у којима је потребна заштита тајних података у ИКТ систему.

Применом мера безбедности ради заштите ИКТ система постижу се следећи ефекти:

- идентификација особа које приступају систему;
- контрола и евиденција приступа на основу датог права приступа из дефинисане базе података;
- обезбеђивање поузданог начина да се укаже на степен тајности;
- идентификација корисника и поуздана евиденција одштампаног, копираног, модификованог или избрисаног тајног податка;
- заштита важних техничких и програмских елемената и функционалност система;
- контрола и управљање руковањем и преносом носача података на којима се чувају тајни подаци;
- планирање, конфигурисање, управљање и контрола мрежних уређаја.

Ове мере заједно чине основу за заштиту ИКТ система од различитих претњи, али је важно континуирано пратити нове трендове и технологије како би се осигурало да су системи увек заштићени од најновијих претњи.

Криптографска заштита ИКТ система у којима се обрађују тајни подаци је део информационе безбедности. Применом криптографских средстава и метода обезбеђује се сигуран и заштићен пренос тајних података у ИКТ системима између две тачке кроз неконтролисани простор. Тиме се значајно повећава безбедност тајних података и смањује могућност њиховог компромитовања и наношења штете.

Криптографске методе и средства примењују се са циљем очувања аутентичности, интегритета и доступности тајних података. Приликом преноса тајних података, сваки ИКТ систем који обрађује тајне податке степена тајности „ПОВЕРЉИВО“ и више треба да буде заштићен од компромитујућег електромагнетног зрачења (КЕМЗ).

Према резултатима мерења спроведених уз помоћ одговарајуће опреме за зонирање објеката и мерења електромагнетног зрачења одређују се безбедносне зоне у објектима у којима се обрађују тајни подаци. У ствари, то значи одређивање просторија према степену заштите од електромагнетног зрачења.

На основу резултата који су добијени мерењима, предузимају се одређене безбедносне мере за смањење електромагнетног зрачења ван контролисаног простора установе, чиме се избегава могућност отицања тајних података путем компромитујућег електромагнетног зрачења опреме.

У области емисионе безбедности, мерења електромагнетног зрачења врше се на опреми која ће се користити за обраду тајних података. На основу добијених резултата утврђује се врста опреме која ће се користити у одговарајућим зонама безбедности. Ова врста безбедносних мера је неопходна, јер се суочавамо са великим ризиком од компромитовања тајних података које емитује ИКТ опрема.

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ
И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

ТЕЛЕФОН: +381 11 361 65 64

e-mail: office@nsa.gov.rs, kontakt@nsa.gov.rs

web: www.nsa.gov.rs