ПОСТУПАЊЕ У СЛУЧАЈУ ИНЦИДЕНТА СА ТАЈНИМ ПОДАЦИМА

Безбедносни инцидент у раду са тајним подацима представља сваки догађај, радњу или пропуст који може угрозити или већ угрожава безбедност тајних података. Ови инциденти обухватају ситуације као што су губитак, крађа, оштећење или неовлашћено откривање података, али и одступања од прописаних мера заштите. У таквим случајевима, обавеза пријаве инцидента од стране свих лица која раде са тајним подацима је од кључне важности. Реакција на инцидент укључује процену ризика, примењивање мера санације и обавештавање надлежних органа, како би се спречиле даље последице и унапредио систем заштите података.

Дефиниција безбедносног инцидента - Безбедносни инцидент у раду са тајним подацима обухвата сваки догађај, радњу или пропуст који доводи или може довести до угрожавања, компромитације или неовлашћеног приступа тајним подацима. То укључује ситуације у којима долази до губитка, крађе, оштећења, уништења или неовлашћеног откривања домаћих или страних тајних података. Безбедносним инцидентом се сматра и свако одступање од прописаних мера заштите утврђених законом, подзаконским актима, безбедносним политикама и интерним процедурама. Овакви инциденти могу настати услед намерних радњи (као што су шпијунажа или злоупотреба овлашћења) или ненамерних пропуста (нехат, немар, техничке грешке), а у оба случаја последице могу бити озбиљне и подложне правној одговорности. Упознавање са појмом и механизмима поступања у случају безбедносног инцидента представља кључни сегмент система заштите тајних података.

Обавеза обавештавања - Сва лица која на било који начин раде са тајним подацима имају неодложну обавезу да пријаве сваки безбедносни инцидент или сумњу на повреду мера заштите. Обавештавање се врши непосредно надређеном, овлашћеном лицу за заштиту тајних података или руководиоцу органа. У зависности од тежине и природе инцидента, обавештавају се и Канцеларија Савета за националну безбедност и заштиту тајних података, службе безбедности (БИА или ВБА у складу са надлежностима) или надлежно тужилаштво. Ова обавеза се заснива на члану 35. став 3. Закона о тајности података и односи се на сва лица која су:

- запослена, ангажована или овлашћена за руковање тајним подацима;
- преносила, обрађивала или чувала податке, чак и ван службених просторија;
- уочила повреду мера као део безбедносног, техничког или организационог система;
- примила пријаву или самостално открила инцидент као овлашћено лице.

Одлагање, прикривање или непријављивање инцидента сматра се тешком повредом обавеза и може водити дисциплинској, прекршајној или кривичној одговорности.

ПОСТУПАЊЕ У СЛУЧАЈУ ИНЦИДЕНТА СА ТАЈНИМ ПОДАЦИМА

Класификација инцидената - У складу са одредбама Закона о тајности података („Сл. гласник РС“, бр. 72/2009), инциденти у систему заштите тајних података класификују се према степену ризика по заштићене интересе и врсти повреде закона. У најширем смислу, свака компромитација штићених података подразумева неовлашћен приступ, откривање, измену, уништавање или губитак података, што представља повреду основних принципа заштите и може довести до озбиљних последица по јавне органе, правна лица или појединце. Компромитација може настати, на пример, када је сеф са тајним подацима остављен отворен и без надзора, када неовлашћено лице има увид у садржај, ако се подаци преносе преко небезбедних канала комуникације или се износе ван службених просторија без адекватне заштите. Повреда може настати и ако се не поштује прописана процедура за уништавање тајних података.

Најчешћи узроци инцидената су људске грешке и немар запослених, недовољна обученост лица која рукују тајним подацима, сајбер напади, злоупотреба додељеног приступа, као и технички пропусти у мерама физичке и техничке заштите. Конкретни ризици укључују ненамерна открића података лицима која немају право да их знају, погрешну конфигурацију система, намерне злоупотребе попут саботаже, шпијунаже или хакерских напада, као и губитак уређаја који садрже тајне податке. Класификација инцидената врши се у односу на потенцијалну или насталу штету по интересе Републике Србије, као и на утицај на интегритет и доступност података. Сврха класификације је процена ризика и приоритизација мера одговора.

Први ниво представља повреду радне дисциплине, када поступање није довело до компромитације података, али је било несавесно или незаконито, као што је непоштовање процедура, немар у примени заштитних мера, непријављивање губитка података или приступ без основе у службеној функцији. У тим случајевима примењују се дисциплинске мере у складу са законом, које могу укључити упозорење, смањење плате, премештај, разрешење или отказ. **Други ниво** подразумева прекршај, када инцидент није довео до компромитације, али указује на озбиљне пропусте у примени мера заштите. Такви случајеви укључују, између осталог, неправилно означавање тајности, изостанак образложења о одређивању тајности, непредузимање мера од стране руковаоца, као и достављање података неовлашћенима без откривања садржаја. За ове прекршаје закон предвиђа новчане казне у распону од 5.000 до 50.000 динара. **Трећи и најтежи ниво** јесте кривично дело, када је дошло или је могло доћи до компромитације тајних података, било неовлашћеним саопштавањем, губитком, откривањем или прибављањем података без одобрења. Закон разликује казне у зависности од степена тајности: за податке означене као „интерно“ или „поверљиво“ предвиђена је казна затвора од 3 месеца до 3 године, за „строго поверљиво“ од 6 месеци до 5 година, а за „државну тајну“ од 1 до 10 година. У тежим облицима, као што су кривична дела почињена из користољубља, у иностранству или у условима ратног стања, казне могу достићи и до 15 година затвора. Ако је дело учињено из нехата, санкције су блаже и крећу се од новчаних казни до пет година затвора, зависно од степена тајности.

ПОСТУПАЊЕ У СЛУЧАЈУ ИНЦИДЕНТА СА ТАЈНИМ ПОДАЦИМА

Оваква класификација омогућава доследно реаговање, примену одговарајућих мера и унапређење безбедносне културе у систему заштите тајних података.

Процена околности и правна квалификација - У складу са Законом о тајности података („Сл. гласник РС“, бр. 72/2009), инциденти у систему заштите тајних података класификују се према степену ризика по заштићене интересе и врсти повреде закона. Компромитација подразумева неовлашћен приступ, откривање, измену, уништавање или губитак података, што нарушава основне принципе заштите и може имати озбиљне последице по јавне органе, правна лица или појединце. Примери компромитације укључују остављање отвореног сефа са поверљивим подацима, увид неовлашћених лица, коришћење небезбедних канала комуникације или непоштовање прописаних процедура за уништавање података. Узроци најчешће проистичу из људске грешке, немара, недовољне обучености, злоупотребе приступа, сајбер напада или техничких пропуста у мерама заштите. Инциденти се процењују и правно квалификују као: – Повреда радне дисциплине, када није дошло до компромитације, али је поступање било несавесно или противзаконито (нпр. непоштовање процедура, приступ без основа); – Прекршај, ако је прекршен закон или прописана процедура без директне компромитације, али са озбиљним пропустима у примени мера заштите (нпр. непотпуно означавање или пропуст у поступању руковаоца); – Кривично дело, када је дошло или је могло доћи до озбиљне компромитације (нпр. неовлашћено откривање, губитак, прибављање података без одобрења).

О тежини инцидента одлучује више фактора: врста и степен тајности података, намера извршиоца, настала или могућа штета и потенцијални утицај на националну безбедност. Погрешна правна квалификација може довести до пропуста у поступању и озбиљних последица. У зависности од квалификације, примењују се различити механизми: – за дисциплинске повреде – интерне мере (упозорење, разрешење, отказ), – за прекршаје – новчане казне, – за кривична дела – казне затвора у распону од три месеца до десет година, а у тежим случајевима и до петнаест година. Процена ризика и последица је суштинска за разумевање степена угрожености. Она мора обухватити не само конкретну штету, већ и могуће импликације по државу, права појединаца или међународне односе.

Поступање у случају инцидента - У случају губитка, крађе, оштећења, уништења или неовлашћеног откривања тајних или страних тајних података, овлашћено лице или старешина органа јавне власти обавезно:

- хитно утврђује околности инцидента и врши процену штете;
- примењује мере санације и спречавања сличних случајева;
- саставља извештај у складу са члановима 36. и 84. Закона о тајности података;
- иницира унутрашњу контролу ради утврђивања узрока и одговорности.

ПОСТУПАЊЕ У СЛУЧАЈУ ИНЦИДЕНТА СА ТАЈНИМ ПОДАЦИМА

Сваки такав инцидент се сматра безбедносним ризиком високог нивоа и захтева брзу, координисану и документовану реакцију. Потребно је одмах обавестити:

1. орган од ког је податак потекао;
2. надлежно тужилаштво и Канцеларију Савета за националну безбедност и заштиту тајних података;
3. Безбедносно-информативну агенцију, ако је инцидент од ширег значаја.

Извештај о инциденту мора да садржи опис догађаја, анализу узрока, процену ризика и предузете мере.

Препоручене мере - Канцеларија Савета за националну безбедност и заштиту тајних података препоручује да сваки орган установи системске мере за превенцију и брз одговор:

- редовне безбедносне провере и анализе ризика;
- континуирану едукацију запослених;
- прецизне процедуре за руковање тајним подацима;
- техничке и организационе мере у ИКТ и другим критичним секторима.

Руковалац тајних података у органу јавне власти или старешина органа играју кључну улогу у управљању инцидентом. Њихове обавезе укључују:

- **Утврђивање чињеница:** у сарадњи са стручњацима идентификују се узроци и околности инцидента (нпр. људска грешка, технички пропуст или злоупотреба);
- **Процена штете:** утврђује се обим и последице инцидента по безбедност, систем и међународне обавезе;
- **Хитне мере:** техничка и организациона санација, обустављање приступа, изолација система;
- **Спречавање понављања:** ревизија процедура, додатне обуке, јачање контролних механизама;
- **Извештавање:** доставља се извештај Канцеларији Савета за националну безбедност и заштиту тајних података о свим мерама и закључцима.

Циљ је системски приступ, усклађен са законом, који обезбеђује поуздану заштиту података и јачање безбедносне културе у институцији.

ПОСТУПАЊЕ У СЛУЧАЈУ ИНЦИДЕНТА СА ТАЈНИМ ПОДАЦИМА

Контролна листа у случају инцидента - Органи јавне власти и правна лица се охрабрују да примењују унапред дефинисану листу за проверу, као алат за брзо и ефикасно реаговање у случају инцидента. Листа треба да обухвати:

- прецизну идентификацију и одређивање врсте и озбиљности инцидента;
- благовремено обавештавање свих релевантних актера и структура;
- детаљну анализу, потпуну документацију догађаја и процену настале штете;
- предузимање корективних мера ради отклањања последица, као и превентивних мера ради спречавања понављања сличних инцидената.

Тиме се обезбеђује координисан и систематски приступ у управљању инцидентима.

На крају - Ефикасно управљање инцидентима са тајним подацима представља не само темељ безбедносне културе, већ и кључни елемент у очувању интегритета и поверења у безбедносне системе. Сви инциденти морају бити обрађени у строгом складу са законом, уз брзу, али пажљиву реакцију, и одлучност организације да минимизира насталу штету. Поред тога, неопходно је спровести свеобухватну процену и применити адекватне корективне и превентивне мере које не само да спречавају поновно настајање инцидената, већ и стално унапређују систем заштите, чинећи га отпорнијим и ефикаснијим у будућности.

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

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

web: www.nsa.gov.rs