ДОПРИНОС ОРГАНИЗАЦИЈЕ НАСТАНКУ ШТЕТНОГ ДОГАЂАЈА СА ТАЈНИМ ПОДАЦИМА

Допринос организације настанку штетног догађаја са тајним подацима често је резултат пропуста који се јављају на системском, оперативном или едукативном нивоу. Организације које не успоставе целовит и функционалан систем заштите тајних података у складу са законским обавезама, излажу се значајним безбедносним ризицима и потенцијалним правним последицама.

Најчешћи **системски пропусти** укључују одсуство званично усвојеног Плана заштите тајних података, непостављање руковаоца тајних података, као организационе јединице или лица одговорног за руковођење системом заштите, као и недостатак јасно дефинисаних унутрашњих аката и процедура за руковање и управљање тајним подацима. Уз то, чест је и недостатак документације о примени мера заштите тајних података. Лоша техничка и физичка инфраструктура — као што су просторије без контроле приступа, непрописно складиштење папирних или електронских података — додатно повећава ризик од инцидената.

Превентивне мере се у многим организацијама – органима јавне власти или правним лицима, недовољно примењују или се формално спроводе без суштинске контроле, како унутрашње тако и спољашне. Неуспостављање планова управљања ризиком, изостанак редовних процена безбедносних претњи и непостојање доследне персоналне безбедности, која обухвата како безбедносне провере лица која приступају тајним подацима, тако и поседовање одговарајућих сертификата за приступ тајним подацима, представљају озбиљне пропусте. Поред тога, коришћење неакредитованих или лоше одржаваних информационо-комуникационих система за рад са тајним подацима који не поседују адекватне криптографске мере, као ни политике ажурирања и техничке контроле, знатно умањује ниво заштите.

Недовољна обученост запослених је чест фактор ризика. Организације често не организују обавезне почетне обуке при пријему у радни однос, не спроводе периодичне обуке у складу са променом прописа или технолошким новинама, нити практичне вежбе симулације инцидената. Изостанак специјализованих едукација за лица са посебним приступом (руковаоци, унутрашња контрола, лица за процену ризика) доводи до тога да постоји озбиљан дисбаланс у знању и компетенцијама. Невођење евиденције о похађању и садржају обука за рад са тајним подацима додатно онемогућава управљање кадровским капацитетима и контролу стручности.

Реакција на инциденте је често неадекватна због непостојања јасно дефинисаних унутрашњих процедура за пријаву, реаговање, истраживање и санирање инцидената у раду са тајним подацима. У пракси, пропушта се дубинска анализа узрока инцидената, не формирају се комисије за процену штете, а евиденција инцидената се не води систематично. Непријављивање инцидената надлежним државним органима, као и одсуство предузимања мера за ублажавање последица, угрожава интегритет система заштите и ствара ризик од понављања истих пропуста.

ДОПРИНОС ОРГАНИЗАЦИЈЕ НАСТАНКУ ШТЕТНОГ ДОГАЂАЈА СА ТАЈНИМ ПОДАЦИМА

Одговорност често није јасно утврђена ни на личном ни на функционалном нивоу. Унутрашњи акти не предвиђају механизме за утврђивање дисциплинске, прекршајне или кривичне одговорности у случају кршења правила о заштити тајних података. Без јасно дефинисаног система санкција и контролних механизама, пропусти остају несанкционисани, што охрабрује небезбедно понашање и повећава ризик од поновног настанка инцидената.

Толерисање културе небезбедног поступања са тајним подацима представља дубоко укорењен проблем. Овакво окружење се карактерише занемаривањем процедура, рутинским заобилажењем правила, недовољном свешћу о ризицима, као и одсуством система за анонимно пријављивање пропуста и неправилности. Запослени у таквом систему не осећају личну одговорност, што доводи до пада безбедносне културе и повећане учесталости инцидената.

Решења за ове проблеме морају бити системска и доследна. Кључне мере укључују: успостављање јасно дефинисаног и функционалног система заштите тајних података, увођење редовних и обавезних обука, имплементацију процедура за реаговање и анализу инцидената, те промовисање културе одговорности и поштовања правила. Лидерство у области безбедности и транспарентност у поступању морају бити подржани механизмима контроле, ревизије и извештавања како би систем функционисао ефикасно и одрживо.

Област пропуста	Кључни проблеми
Системска организација	Недостаје план заштите тајних података, руковалац тајних података, одговорна лица, процедуре, техничка/физичка заштита
Превентивне мере	Нема процене ризика, сертификата за приступ тајним подацима, акредитованих ИКТ система за рад са тајним подацима
Обука и едукација	Недовољно или формално спровођене обуке, без евиденције и специјализације
Реакција на инциденте	Нема поступка за пријаву и анализу инцидената, непријављивање надлежнима
Одговорност	Непостојање механизама за дисциплинску, прекршајну или кривичну одговорност, несанкционисани пропусти
Безбедносна култура	Толерише се небезбедно понашање, занемарују се процедуре, нема система за пријаве (негативан контекст „цинкарење“)

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

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

web: www.nsa.gov.rs