СИСТЕМСКИ, ТЕХНОЛОШКИ И ПСИХОЛОШКИ АСПЕКТИ ЗАШТО ЗАПОСЛЕНИ КРШЕ ПРОЦЕДУРЕ У РАДУ СА ТАЈНИМ ПОДАЦИМА?

Системски аспекти у раду са тајним процедурама - Посебан изазов у домену заштите тајних података представља такозвани „ресорски модел“, који се у пракси ослања на наслеђене „добре праксе“ уместо на јасно дефинисане прописе. Овај модел функционише као неформални механизам, произашао из традиције правних и политичких система који су постојали на простору Србије – од Краљевине Србије и Југославије, преко СФРЈ и СРЈ, па све до савремених система. Уместо усклађеног, национално кодификованог приступа, органи јавне власти често примењују различите методе заштите података, у зависности од ресора, историје институције или спољашњих утицаја. Додатни проблем лежи у томе што су бројни механизми заштите података у Србији формулисани кроз п**ројекте и иницијативе међународних организација**, које су – вођене својим националним моделима – „пресликале“ сопствене стандарде на домаће институције. Такав приступ често доводи до неусаглашености међу органима јавне власти, неједнаке примене правила и слабљења целокупне безбедносне инфраструктуре. Уместо универзално обавезујућег система, настаје мрежа ресорских аутономија у којој недостају јасна вертикална контрола, одговорност и ефикасна размена информација. Решење лежи у изградњи националног модела заштите, заснованог на савременим потребама и усклађеном са реалним институционалним капацитетима.

Недостаци техничке инфраструктуре – ИКТ системи без заштите - Озбиљан проблем у раду са тајним подацима у Републици Србији представља недостатак јединствених техничких стандарда у државним институцијама. Док поједине установе користе савремене системе са мултифакторском аутентификацијом и аутоматским евиденцијама приступа, друге се и даље ослањају на застареле софтвере без основне заштите. Посебну тешкоћу ствара некомпатибилност међу системима, која онемогућава безбедну размену података и присиљава запослене на импровизована и небезбедна решења, попут употребе јавних мејл сервиса. Додатни ризик представља неконтролисана употреба преносивих уређаја, као што су USB меморије и лаптопови, који нису заштићени од крађе или губитка података. Иако формално постоје прописана правила о акредитацији ИКТ система, она се у пракси ретко примењују због високих трошкова или недостатка стручног кадра. Овим проблемима додатно доприноси и недостатак националног акредитационог тела које би надгледало примену стандарда и обавезу безбедносне процене ИКТ инфраструктуре на нивоу целе државне управе. Једно од решења је увођење редовних безбедносних ревизија и централизована модернизација ИКТ система, како би се обезбедила уједначена техничка заштита у свим институцијама.

Технолошки аспекти заштите тајних података: Пропусти и ризици - Иако Закон о информационој безбедности и прописи који уређују рад са дигиталним документима постављају оквире за управљање тајним подацима, у пракси се често јављају проблеми због непотпуне или погрешне примене. Један од кључних изазова је непостојање класификације нивоа тајности, што доводи до тога да се подаци различите осетљивости чувају у истим системима, без одговарајуће техничке заштите.

СИСТЕМСКИ, ТЕХНОЛОШКИ И ПСИХОЛОШКИ АСПЕКТИ ЗАШТО ЗАПОСЛЕНИ КРШЕ ПРОЦЕДУРЕ У РАДУ СА ТАЈНИМ ПОДАЦИМА?

Честа грешка је коришћење неакредитованих ИКТ система који немају сертификате за рад са поверљивим информацијама, што их чини рањивим на сајбер-нападе и злоупотребу. Неки органи јавне управе и даље користе облачне сервисе и мејлинг листе без енкрипције за размену осетљивих докумената, упркос јасним прописима. Додатни проблем представља погрешна примена прописа који се односе на управљање такозваним „отвореним подацима“, а који се у пракси користе и за рад са тајним информацијама, нарочито у локалним самоуправама и институцијама које нису директно повезане са националном безбедношћу и одбраном. То доводи до неадекватног архивирања дигиталних докумената, који се често складиште на несигурним серверима или приватним уређајима запослених. Недостатак централизованог система за управљање тајним подацима онемогућава ефикасну контролу приступа и откривање неовлашћеног коришћења. Решење лежи у строжој примени постојећих прописа, редовним безбедносним ревизијама ИКТ система и увођењу аутоматизованих алата за класификацију и заштиту података, како би се смањио утицај људског фактора у кршењу процедура.

Психолошки аспекти одступања у раду са тајним подацима - Упркос строгим прописима, у пракси се често појављују пропусти који угрожавају безбедносну културу. Узроци не леже увек у намерном кршењу правила, већ у психолошким и организационим факторима:

- **Рутина и навика** – Игнорисање процедура из навике, услед понављања истих задатака.
- **Претерано самопоуздање** – Вера да грешке не могу да се десе баш њима, води ка непотребном ризику.
- **Страх од конфронтације** – Избегавање пријављивања неправилности због хијерархије и страха од последица.
- **Стрес и рокови** – Под притиском посла, безбедносне мере падају у други план.
- **Недовољна свест о последицама** – Мањак континуиране едукације доводи до потцењивања ризика.

Ови фактори указују на потребу да се питање безбедности не сведе само на формално поштовање прописа, већ да постане тема системског деловања, континуиране едукације и културне трансформације унутар институција. Сагледавајући свакодневну праксу у органима јавне власти и правним лицима који рукују са тајним подацима, издвајају се бројни фактори који суштински доприносе нарушавању безбедносних процедура:

1. **Илузија безопасности као психолошка претња заштити тајних података** - Запослени понекад умањују значај докумената, верујући да „ово неће ником нашкодити“, што доводи до игнорисања безбедносних процедура. Такав став се често базира на претходним искуствима без последица, чиме се развија лажни осећај сигурности и нормализује ризично понашање.

СИСТЕМСКИ, ТЕХНОЛОШКИ И ПСИХОЛОШКИ АСПЕКТИ ЗАШТО ЗАПОСЛЕНИ КРШЕ ПРОЦЕДУРЕ У РАДУ СА ТАЈНИМ ПОДАЦИМА?

Конкретне последице овог начина размишљања укључују: немарно поступање са тајним подацима (неконтролисано умножавање, непрописно уништавање, остављање на непокривеним местима) и разговоре о тајним и осетљивим информацијама ван одговарајућих просторија (ходници, кафетерије, јавни простори).

Овакав приступ представља озбиљну и често невидљиву претњу за интегритет система. Превенција мора обухватити едукацију, подизање свести и критичко преиспитивање уврежених ставова.

2. **Преоптерећеност и временски притисак као фактори заобилажења безбедносних процедура** - Запослени често стављају брзину испред сигурности, верујући да је важније „завршити посао на време“ него поштовати формалне безбедносне кораке. Страх од кашњења, санкција или губитка поверења подстиче ризичне одлуке, попут:

- слања тајних података преко несигурних канала (нпр. необезбеђена е-пошта или апликације без шифровања)
- коришћења приватних, непријављених уређаја за приступ тајним подацима и информацијама

Овакво понашање указује на системски проблем — несагласност између радне динамике и безбедносних захтева. Превенција подразумева техничка побољшања, али и промену свести о значају времена у контексту безбедности и сигурности.

3. **Социјални притисак и конформизам као претња безбедности података** - Запослени често прилагођавају своје поступке понашању већине или очекивањима надређених, што доводи до нормализације кршења процедура. Изрази попут „сви то раде“ или „шеф је рекао да је у реду“ подстичу пасивно прихватање небезбедног понашања и урушавање одговорности. Типичне последице:

- колективна толеранција на кршење правила, без критичког преиспитивања
- игнорисање упозорења и смерница безбедносних механизама

Социјална динамика унутар организације обликује безбедносну културу. Зато је неопходно да интервенције укључе читаве тимове и руководиоце који промовишу одговорно понашање.

4. **Недовољна свест о последицама као ризик за безбедност тајних података** - Запослени понекад потцењују вредност поверљивих информација, верујући да „нису интересантне трећим странама“. Тај став води ка занемаривању безбедносних процедура и одустајању од личне одговорности, што умањује ангажовање и повећава ризик од пропуста. Типичне последице:

- остављање тајних докумената на неконтролисаним, видљивим местима
- усмено дељење лозинки и тајних података без проверене потребе и идентитета

СИСТЕМСКИ, ТЕХНОЛОШКИ И ПСИХОЛОШКИ АСПЕКТИ ЗАШТО ЗАПОСЛЕНИ КРШЕ ПРОЦЕДУРЕ У РАДУ СА ТАЈНИМ ПОДАЦИМА?

Овај облик небриге не сме постати културна норма. Јачање свести и личне одговорности је кључни корак у заштити система од реалних претњи.

5. **Осећај безнађа и апатије као фактор небезбедног поступања** - Дуготрајан рад у нефункционалном систему може изазвати апатију и губитак мотивације код запослених. Ставови попут „ништа не мењам“ или „свеједно је шта радим“ указују на психолошко дистанцирање и губитак осећаја одговорности. Ако систем не реагује на инциденте, мере безбедности се доживљавају као формалност, што додатно погоршава ситуацију. Последице оваквог става:

- намерно игнорисање правила, чак и када је ризик очигледан
- нарушавање физичке контроле, попут уноса личних уређаја у заштићене зоне без дозволе

Решење захтева обнову поверења кроз транспарентност, доследну примену прописа и активно укључивање запослених у креирање реалних решења.

Како побољшати безбедносну културу у раду са тајним подацима

1. Обуке засноване на реалним сценаријима

- Симулације инцидената и вежбе са ризичним ситуацијама
- Развијање практичних вештина и навика реаговања

2. Баланс између санкција и мотивације

- Доследно кажњавање прекршаја, без изузетака
- Подстицаји за одговорно понашање и превентивно деловање

3. Промена организационе културе

- Неформални разговори о безбедности као део свакодневнице
- Безбедност као тема редовних састанака и тимске одговорности

4. Анонимни систем за пријављивање пропуста

- Механизми за сигурно и поверљиво пријављивање
- Заштита пријављивача и подршка храбрим појединцима

СИСТЕМСКИ, ТЕХНОЛОШКИ И ПСИХОЛОШКИ АСПЕКТИ ЗАШТО ЗАПОСЛЕНИ КРШЕ ПРОЦЕДУРЕ У РАДУ СА ТАЈНИМ ПОДАЦИМА?

Системски приступ заштити тајних података - Кршење безбедносних процедура често није појединачан чин неодговорности, већ резултат психолошких слабости, организационих пропуста и мањкавости у комуникацији. Рад са тајним подацима захтева свеобухватан приступ који превазилази формалне прописе. Кључни кораци за побољшање:

- **Интеграција безбедности у радну организацију** - Безбедносне процедуре треба да буду природно уклопљене у свакодневне активности, без да се доживљавају као терет.
- **Практична и реалистична обука** - Вежбе засноване на симулацијама стварних ризика помажу у развоју навика и брзих, свесних реакција.
- **Јасна и доследна подршка руководства** - Руководиоци морају недвосмислено показати да је безбедност приоритет, а не формалност — кроз пример, подршку и доследност.

Порука: Иако је лична одговорност важна, стварне и одрживе промене настају када цео систем обезбеђује подршку, јасна правила и истинску мотивацију.

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

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

web: www.nsa.gov.rs