ПРИМЕРИ ЛОШЕ ПРАКСЕ СИСТЕМА РАДА СА ТАЈНИМ ПОДАЦИМА

1. Приступ тајним подацима без институционалног оквира и организационе безбедности -кривично дело из члана 98. Закона о тајности података

2. Третирање тајних података и докумената као отворених и личних података - кривично дело из члана 98. Закона о тајности података

3. Запослени без сертификата приступају тајним подацима - кривично дело из члана 98. Закона о тајности података

4. Лица без овлашћења старешине органа јавне власти креирају тајне податке - прекршај из члана 99. тачка 11. Закона о тајности података

5. Непостојање процедура имплементације Закона о тајности података - прекршај из члана 99. тачка 11. Закона о тајности података

6. Рад са тајним подацима на информационим системима који су прикључени на интернет- прекршај из члана 99. тачка 11. Закона о тајности података

7. Неуспостављање простора (безбедносних зона) за чување тајних података и ненабављање одговарајуће опреме - прекршај из члана 99. тачка 11. Закона о тајности података

8. Спровођење поверљивих набавки без утврђене процедуре рада са тајним подацима и уступање тајних података правним лицима без одговарајућег сертификата (безбедносне акредитације простора и запослених) - кривично дело из члана 98. Закона о тајности података; прекршај из члана 99. тачка 11. Закона о тајности података

9. Објављивање тајних података у медијима без процедуре скидања ознаке тајности- кривично дело из члана 98. Закона о тајности података

10. Непостојање функционалног руковаоца тајних података и система унутрашње контроле рада са тајним подацима у органу јавне власти - прекршај из члана 99. тачка 16. Закона о тајности података; прекршај из члана 99. тачка 11. Закона о тајности података (везује се за члан 32. став 1. тачка 5. Закона о тајности података)

ПРИМЕРИ ЛОШЕ ПРАКСЕ СИСТЕМА РАДА СА ТАЈНИМ ПОДАЦИМА

11. Непрописно означавање тајних података, без одговарајуће одлуке и без критеријума за одређивање тајности – прекршај из члана 99. тачка 3. Закона о тајности података

12. Неуспостављање система едукација у раду са тајним подацима на нивоу органа јавне власти - прекршај из члана 100. Закона о тајности података

13. Несистематизовање радних места која имају приступ тајним подацима у органу јавне власти - прекршај из члана 99. тачка 11. Закона о тајности података

14. Прослеђивање тајних података другим органима јавне власти без одговарајуће процедуре „ПОТРЕБНО ПОДЕЛИТИ СА“ и без курирске доставе - прекршај из члана 99. тачка 11. Закона о тајности података (везује се за члан 32. став 1. тачка 3. Закона о тајности података)

15. Разговор о тајним подацима са лицима која нису сертификована и изван одговарајуће безбедносне зоне (нпр. у ресторану, на улици, у ходнику или тоалету...) - кривично дело из члана 98. Закона о тајности података

16. Увођење страних држављана у административне или безбедносне зоне без одлуке старешине органа јавне власти - кривично дело из члана 98. Закона о тајности података

17. Уступање тајних података непозваним лицима, без одговарајуће процедуре и одлука – кривично дело из члана 98. Закона о тајности података

18. Уношење мобилних телефона, лаптопова, усб-ова и слично у безбедносне зоне без процедуре и одобрења - прекршај из члана 99. тачка 11. Закона о тајности података

ПРИМЕРИ ЛОШЕ ПРАКСЕ СИСТЕМА РАДА СА ТАЈНИМ ПОДАЦИМА

Највећи ризици лоших пракси су:

1. **Неадекватна заштита тајних података:** Поступање са тајним подацима без претходно имплементираног система заштите тајних података који подразумева (персоналну безбедност, физичку безбедност, административну безбедност, индустријску безбедност, информациону гаранцију и контролу и надзор) кумулативно представља стварање услова за одавање тајних података. Полазећи од појма тајног по датка неимплементирање система заштите тајних података директно утиче на угрожавање националне безбедности Републике Србије.

2. **Неовлашћен приступ и коришћење тајних података:** За систем заштите тајних података од нарочитог значаја је превентивно планирање, предвиђање, организовање и реализовање стратегијских, нормативних и организацијских услова за рад са тајним подацима. У начелу органи јавне власти морају утврдити степен тајности података којима располажу, начин приступа тајним подацима (да ли се добијају или креирају), анализу радних места која подразумева рад са тајним подацима и адекватну селекцију лица. Овакав приступ за услов има доношење јасних процедура које намећу искључивање произвољности у раду са тајним подацима.

3. **Неадекватна обука и едукација.** Кадровима који раде са тајним подацима поред механизма безбедносне провере мора се посебна пажња усмерити на едукације и обуке, као неизоставном битном елементу система заштите тајних података. Едукација и високо квалитетна обука се спроводи пре свега у циљу развијања и усавршавања њихових способности, знања, вештина на дугорочном плану, како би били што професионалнији, успешнији и ефикаснији у оквиру својих радних места. Таквим приступом и процедурама битно би се смањила опасност од несавесног чувања и одавања тајних података.

ПРИМЕРИ ЛОШЕ ПРАКСЕ СИСТЕМА РАДА СА ТАЈНИМ ПОДАЦИМА

4. **Нехатно и немарно поступање са тајним подацима, као и несавестан пренос тајних података**: Ово се може демонстрирати нарочито у канцеларијском пословању у раду са тајним подацима, и суштински представља најугроженији сегмент система заштите тајних података. Неки од негативних примера праксе: неправилност приликом одређивања тајних података, степена тајности, кршења процедура у завођењу, пријему, слању, паковању, непостојање курирског уверења, обрасца о извршеној примопредаји тајног податка, раздуживање предмета, уништавање, копирање итд.

5. **Непоштовање процедура о физичко-техничким мерама заштите:** Рад са тајним подацима могућ је искључиво у рестриктивним зонама (административна /ИНТЕРНО/ и безбедносна /ИНТЕРНО/ПОВЕРЉИВО/СТРОГО ПОВЕРЉИВО/ДРЖАВНА ТАЈНА). Непоштовање процедура огледа се у следећим примерима: када се непозваном лицу омогући улазак у зону, када се омогући употреба рачунара, рачунарске мреже (неправилност у случају одржавања), пропусти у избору администратора, корисника, уношење мобилних телефона, губљење преносних уређаја или неправилна употреба, омогућавање снимања објеката, непоседовање сефа, касе, решетки, система рестриктивног приступа, непоштовање процедура пп заштите итд...

Све горе наведено указује на значај едукација и постојање процедура, нарочито имајући у виду да је најслабија карика система заштите тајних података сам човек.

ПРИМЕРИ ЛОШЕ ПРАКСЕ ПОРЕД КРИВИЧНОГ ДЕЛА И ПРЕКРШАЈА ПРЕДСТАВЉАЈУ И УГРОЖАВАЊЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ РЕПУБЛИКЕ СРБИЈЕ.

НА ГРЕШКАМА ДРУГИХ СЕ УЧИ,
ЗБОГ СВОЈИХ ГРЕШАКА СЕ ОДГОВАРА !
ЕДУКУЈТЕ СЕ !

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

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

web: www.nsa.gov.rs