Врз основа на член 68 ставови (2) и (3) од Законот за следење на комуникациите („Службен весник на РСМ, бр. 71/2018 и 108/2019 година), директорот на Оперативно-техничката агенција Скопје донесе

ПРАВИЛНИК

за мерките и стандардите за информациска безбедност кои се должни да ги применуваат операторите на јавни електронски комуникациски мрежи и/или услуги во врска со обврските за спроведување на мерките за следење на комуникациите

I. ОПШТИ ОДРЕДБИ

Предмет на уредување
Член 1

Со овој Правилник се пропишуваат мерките и стандардите за информациска безбедност на информациските системи кои се должни да ги применат операторите на јавни електронски комуникациски мрежи и/или услуги во врска со нивните обврски за спроведување на мерките за следење на комуникациите во согласност со Законот за следење на комуникациите.

Обврски на операторите
Член 2

Операторите на јавни електронски комуникациски мрежи и/или услуги се должни да ги спроведуваат мерките и стандардите за информациска безбедност, во согласност со одредбите од овој Правилник.

Цел на мерките и стандардите за информациската безбедност
Член 3

Со овој Правилник се воспоставуваат безбедносни мерки и стандарди со кои ќе се обезбеди доверливост, интегритет и достапност на информациите.

II. МЕРКИ И СТАНДАРДИ ЗА ИНФОРМАЦИСКА БЕЗБЕДНОСТ

Извештаи на операторите за извршени редовни интерни контроли
Член 4

(1) Операторите вршат редовни интерни проверки за функционирањето, ефектите и слабостите во безбедноста на информациските системи и за тоа изготвуваат писмени извештаи.
(2) Извештаите од став (1) се даваат на увид на барање на Комисијата за стручен надзор на работата над операторите (во понатамошниот текст Комисијата).
(3) Операторите се должни да ги достават на увид на членовите на Комисијата записниците од редовните извршени надзори од страна на Дирекцијата за заштита на личните податоци, Агенцијата за електронски комуникации и Дирекцијата за безбедност на класифицирани информации.

Одредување одговорно лице за примена на мерките и стандардите за информациска безбедност

Член 5

Операторите на јавни електронски комуникациски мрежи и/или услуги се должни да одредат лице одговорно за примена на мерките и стандардите за информациска безбедност.

Обврски на одговорното лице за примена на мерките и стандардите за информациска безбедност

Член 6

Одговорното лице за примена на мерките и стандардите за информациска безбедност:

- врши координација на сите безбедносни активности во однос на воспоставување и одржување информациска безбедност;
- управува со периодичните процени на ризиците за информацискатa безбедност;
- врши редовна процена на ризиците и ажурирање на плановите за справување со приоритетните ризици;
- ја ажурира евиденцијата на закани и потенцијални ризици;
- го координира спроведувањето безбедносни контроли и ја набљудува нивната ефикасност;
- предлага политика и упатства за постигнување безбеден информациски систем;
- учествува во подготвувањето на интерните акти, технички и дополнителни комплементарни политики со кои се обезбедува спроведување на политиката и упатствата за безбеден информациски систем;
- го надгледува спроведувањето на интерните акти за безбедност на информацискиот систем;
- врши внатрешна координација и истрага на настаните што ја загрозиле безбедноста на информацискиот систем, вклучувајќи и соработка со надворешни органи и други институции;
- предлага мерки за надминување на последиците и спречување слични инциденти;
- соработува со одговорните лица за безбедност на информациските системи во ОТА;
- поднесува барање за покренување постапка за утврдување одговорност за повреда на правила за безбедност на информацискиот систем.

Стандарди и правила за безбедност на информациските системи

Член 7

Стандардите и правилата за безбедност на информациските системи опфаќаат:

- минимални критериуми и безбедносни мерки, кои треба да ги исполнуваат информациските системи;
- минимални општи насоки за заштита на информациите од намерни и ненамерни неавторизирани промени, уништување или откривање;
- користење на безбедносните стандарди од серијата МКС ISO/IEC 27000 во информациските системи;
- редовна проверка на безбедноста на информациските системи;
- редовна процена на ризиците поврзани со безбедноста на информациските системи, нивен приоритет, како и мерки за справување со ризиците во случај на нивна појава;
- управување со инциденти поврзани со информацискатa безбедност;
- надлежност и одговорност за воведување, управување и надзор на безбедноста на информациските системи.

Мерки за информациска безбедност на информациските системи

Член 8

Мерки за информациска безбедност на информациските системи што се должни да ги применат операторите на јавни електронски комуникациски мрежи и/или услуги во врска со нивните обврски за спроведување на мерките за следење на комуникациите во согласност со Законот за следење на комуникациите се:

1. Неискористените услуги и протоколи мора да бидат деактивирани;
2. Достапноста на сервисите мора да се ограничи;
3. Неискористениот софтвер мора да се деинсталира (не е дозволено да се инсталира софтвер на систем што не е потребен за работа, одржување или функција на системот);
4. Неискористените функции на оперативниот софтвер и хардвер мора да бидат деактивирани;
5. Софтверските и хардверските компоненти кои го достигнале крајот на животниот век или немаат договор за поддршка не смее да се користат;
6. Појавените слабости во софтверот и хардверот на системот мора да бидат фиксирани или заштитени од злоупотреба;
7. Податоците со потреба од заштита мора да бидат заштитени од неовластено прегледување и манипулација за време на преносот и складирањето;
8. Чувствителни информации (информациите поврзани со електронско следење на комуникациите) не смее да бидат содржани во датотеки или пораки кои се достапни на неовластени корисници;
9. Системите мора да бидат стабилни против ситуации со преоптоварување (мора да се избегне делумно или целосно оштетување на достапноста на системите, при т.н. DoS напади);
10. Системот мора да биде стабилен против неочекувано внесување податоци;
11. Без успешна автентикација и авторизација не смее да се дозволи пристап до функции и информации на системите;
12. Мора да се користат кориснички сметки што овозможуваат недвосмислена идентификација на корисникот;
13. Корисничките сметки мора да бидат заштитени од неовластена употреба со најмалку еден атрибут за автентикација;
14. Корисничките сметки со широки права мора да бидат заштитени со два атрибути за автентикација;
15. Предефинираните и неискористени кориснички сметки мора да бидат избришани или оневозможени;
16. Предефинираните атрибути за автентикација мора да бидат избришани или оневозможени;
17. Привилегиите за корисничките сметки и апликации мора да се намалат на минимум потребен за задачите што треба да ги извршат;
18. Системот мора да биде поврзан со централен систем за администрација на корисници;
19. Сесиите мора да бидат заштитени од киднапирање (употреба на криптографски методи, заштитни мерки на мрежно, транспортно, апликативно ниво);
20. Системот мора да има функција што дозволува најавен корисник да се одлогира во кое било време;
21. Системот мора да има функција што дозволува активна сесија да се прекине автоматски по одредено време на неактивност;
22. Ако се користи лозинка како атрибут за проверка, таа мора да има најмалку осум карактери и да содржи три од следниве категории: големи букви, мали букви, броеви и специјални знаци;

23. Ако се користи лозинка како атрибут за проверка, мора да се спроведат мерки за заштита од насилни напади кои го попречуваат погодувањето на лозинката;
24. Ако се користи лозинка како атрибут за проверка, таа мора да биде скриена кога се прикажува на екранот;
25. Податоците за логирање релевантни за безбедноста мора да бидат испратени до надворешен систем (во соодветни дадотеки) директно по нивното создавање;
26. Да се обезбеди бекап на мрежните елементи со LI функционалност;
27. Системите мора да се приклучени на редудантен систем на напојување со електрична енергија;
28. Системите мора да бидат заштитени од елементарни непогоди и надворешни влијанија.

Одржување на информацискиот систем

Член 9

Физичките или правните лица кои вршат одржување на информациските системи на операторите треба да ги применуваат прописите за информациска безбедност пропишани со овој Правилник.

Физичка сигурност на системите

Член 10

(1) Системите кои се инволвирани во процесот на следење на комуникациите кај операторите треба да се физички лоцирани во безбедносни простории.
(2) Физички пристап до просторијата во која се сместени системите може да имаат само лица со посебни овластувања.
(3) Доколку е потребен пристап на друго лице до просториите каде што се сместени системите, тогаш тоа лице треба да биде придружувано и надгледувано од лице од став (2) на овој член.
(4) Просторијата во која се сместени серверите се заштитува од ризиците во опкружувањето преку примени на мерки и контроли со кои се намалува ризикот од потенцијални закани, вклучувајќи кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

III. НАЧИН НА УПРАВУВАЊЕ СО ИНЦИДЕНТИ

Управување со инциденти

Член 11

Операторите треба да воспостават тим за управување со инциденти поврзани со информацискатa безбедност и да воспостават процедури за следење и управување со безбедносни инциденти.

Правила за управување со безбедносни инциденти

Член 12

Тимот за управување со безбедносни инциденти подготвува Правила за управување со безбедносни инциденти кои треба да ги содржат следните елементи:

- список на идентификувани важни функции на системот и приоритетите за обновување на функционалностите на системот;
- список на идентификувани ресурси кои се неопходни за исполнување на критично важните функции;
- список на можните инциденти со веројатности за нивно појавување, произлегувајќи од оцените на ризикот;

- разработени стратегии за обновување на функционалноста на системот;
- дефинирани мерки за реализација на стратегиите.

Евидентирање и чување документација за информациските системи

Член 13

Одговорното лице за примена на мерките и стандардите за информациска безбедност треба да ја евидентира и да ја чува целокупната документација за информациските системи на операторите и за сите нивни промени.

IV. ЗАВРШНИ ОДРЕДБИ

Член 14

Овој Правилник влегува во сила на денот на неговото донесување.

Директор
Зоран Ангеловски

27.8.2019 година
Скопје