Врз основа на член 47 став 1 точка 6 од Законот за Народната банка на Република Северна Македонија („Службен весник на Република Северна Македонија" бр. 158/10, 123/12, 43/14, 153/15, 6/16, 83/18 и „Службен весник на Република Северна Македонија" бр. 110/21) и член 123 став 9 од Законот за платежни услуги и платни системи („Службен весник на Република Северна Македонија" бр. 90/22), Советот на Народната банка на Република Северна Македонија донесе

О Д Л У К А
за сигурносните мерки за оперативните и сигурносните ризици поврзани со платежните услуги

I. ОПШТИ ОДРЕДБИ

1. Со оваа одлука поблиску се пропишуваат барањата коишто давателите на платежните услуги во согласност со Законот за платежни услуги и платни системи (во натамошниот текст: Законот) се должни да ги исполнат со цел:
   - да воспостават сигурносни мерки за намалување на оперативните и сигурносните ризици поврзани со платежните услуги, преку воспоставување рамка за управување со оперативните и сигурносните ризици,
   - потврда на ефективноста на воспоставените сигурносни мерки преку воспоставување рамка за тестирање и
   - постојана обука и поддршка на корисниците на платежните услуги, заради подигнување на свесноста за сигурносните ризици при извршувањето на платежните услуги.

II. ДЕФИНИЦИИ

2. Одделни изрази употребени во оваа одлука го имаат следново значење:

2.1 **„Рамка за управување со оперативните и сигурносните ризици"** е општа рамка за прифатливото ниво на оперативните и сигурносните ризици поврзани со платежните услуги којашто го опфаќа севкупниот пристап (стратегии, политики, правила, практики, контроли, процеси, системи и слично) за дефинирање, известување и следење на прифатливото ниво на ризик.

2.2. **„Прифатливо ниво на ризик"** е збирно ниво на оперативни и сигурносни ризици поврзани со платежните услуги коишто институцијата е подготвена да ги преземе во рамките на својот капацитет за преземање ризици во согласност со деловниот модел за успешно остварување на своите стратегиски цели.

2.3. **„Длабинска одбрана"** е тип на одбрана со која се воспоставува повеќе од една сигурносна заштитна контрола или контролен механизам којашто

покрива ист ризик и којашто служи како дополнителна сигурносна заштита на претходните механизми.

2.4. **„Неопходност од пристап"** е минимален сет доделени привилегии за пристап заради остварување на потребните активности, како и пристап до потребните податоци неопходни за успешно спроведување на деловниот процес.

III. СИГУРНОСНИ МЕРКИ ЗА ОПЕРАТИВНИ И СИГУРНОСНИ РИЗИЦИ

3. За воспоставување на сигурносните мерки за оперативни и сигурносни ризици, давателите на платежните услуги се должни да воспостават рамка за управување со оперативните и сигурносните ризици, соодветна и пропорционална на природата, обемот и сложеноста на активностите поврзани со давањето на платежната услуга.

4. Рамката од точка 3 од оваа одлука, треба да биде одобрена од органот на управување на давателот на платежната услуга и треба да се ревидира најмалку еднаш годишно, во зависност од промените во опкружувањето и измени на профилот на ризичност.

   Давателите на платежните услуги се должни да обезбедат соодветна документираност на рамката за управување со оперативните и сигурносните ризици при нејзината примена.

5. Рамката за управување со оперативните и сигурносните ризици најмалку содржи:
   - политика за сигурност;
   - прифатливото ниво на ризик;
   - клучните улоги и одговорности, во согласност со точка 7 од оваа одлука, неопходни за спроведување на сигурносните мерки, управување со сигурносните и оперативните ризици и линии на известување;
   - процесите на идентификација, мерење, следење и управување со ризиците коишто произлегуваат од активностите на давателите на платежните услуги поврзани со плаќањето, вклучувајќи и обезбедување непрекинатост во деловното работење;
   - процедури за управување со оперативните и сигурносните инциденти.

6. Давателите на платежните услуги се должни да проверат дали има потреба од промена или унапредување на рамката за управување со оперативните и сигурносните ризици, пред значајни промени во инфраструктурата, процесите или постапките, како и по секој настанат утврден значаен оперативен или сигурносен инцидент, веднаш без непотребно одлагање.

7. Давателите на платежните услуги се должни да воспостават ефективен модел за управување со ризиците, за идентификација и соодветно управување со оперативните и сигурносните ризици преку воспоставување три ефективни линии на одбрана (оперативна, управување со ризик и внатрешна ревизија).

Трите линии на одбрана од став 1 на оваа точка треба да се одделни и меѓусебно независни, да имаат доволно ресурси, јасно определени овластувања и дефинирани постапки за известување до органите на управување или надзор.

8. Давателите на платежните услуги се должни да обезбедат ефективност и ефикасност на сигурносните мерки при користењето услуги од надворешно лице.

   Во договорите со надворешните лица, давателите на платежните услуги треба да го дефинираат потребното ниво на квалитет на бараната услуга, како и да вклучат соодветни сигурносни мерки коишто одговараат со критичноста, значајноста и карактеристиките на услугата којашто ја пренесува давателот на платежната услуга кон надворешното лице.

   Давателите на платежните услуги должни се да го следат нивото на усогласеност на надворешните лица, со нивната рамка за управување со оперативните и сигурносните ризици.

Идентификација и евидентирање на функциите, процесите и средствата

9. Давателите на платежните услуги се должни да ги утврдат и редовно да ги ажурираат своите деловни функции, клучните улоги на извршителите на деловните функции и процесите за поддршка на деловните функции во посебен регистар за таа намена, заради нивно целосно евидентирање, утврдување на нивната значајност и меѓусебна поврзаност со оперативните и сигурносните ризици.

10. Давателите на платежните услуги се должни да ги утврдат и редовно да ги ажурираат информациските системи коишто ги користат, системите за комуникациска технологија, конфигурациите, нивната меѓусебна поврзаност со други внатрешни и надворешни ИТ-системи, заради нивно целосно евидентирање во регистарот и соодветно управување со клучните деловни функции и процеси од точка 9.

Класификација на функциите, процесите и средствата

11. Давателите на платежните услуги должни се да ги класифицираат евидентираните деловни функции, процеси за поддршка и информациски средства од регистарот од точка 9, согласно нивната критичност.

Проценка на ризиците поврзани со функциите, процесите и средствата

12. Давателите на платежните услуги се должни постојано да ги следат заканите и ранливостите, како и редовно да ги ревидираат сценаријата поврзани со ризици коишто влијаат на деловните функции, критичните процеси и информациските средства.

    Давателите на платежните услуги се должни да спроведуваат сеопфатна оцена на изложеноста на оперативните и сигурносните ризици поврзани со платежните услуги коишто ги даваат и на соодветноста на применетите

мерки и контролни механизми за управување со оперативните и сигурносните ризици.

Давателите на платежните услуги се должни да достават ажурирана и сеопфатна оцена на изложеноста на оперативните и сигурносните ризици од став 2 на оваа точка, до Народната банка, најмалку еднаш годишно, а на барање на Народната банка и во пократки временски интервали.

Давателите на платежните услуги се должни да спроведуваат делумни процени на ризиците пред воведувањето значајни промени во инфраструктурата, процесите или постапките коишто влијаат врз сигурноста на платежните услуги.

13. Врз основа на спроведената процена на ризиците од точка 12 од оваа одлука, давателите на платежните услуги се должни да ја утврдат соодветноста на применетите сигурносни мерки и контролни механизми, како и потребата за нивно унапредување.

Примена на сигурносни мерки

14. Давателите на платежните услуги се должни да воспостават и да спроведат превентивни сигурносни мерки, за заштита од утврдените оперативни и сигурносни ризици.

    Мерките од став 1 на оваа одлука треба да обезбедат ниво на сигурност, во согласност со утврденото прифатливо ниво на ризик.

15. Давателите на платежните услуги се должни да воспостават и да спроведат сигурносни мерки во повеќе слоеви, односно да се користи пристапот на т.н. „длабинска одбрана".

16. Давателите на платежните услуги се должни да обезбедат доверливост, интегритет и расположливост на своите критични информациски и комуникациски средства, како и на чувствителните податоци за плаќања.

17. Давателите на платежните услуги се должни постојано да го следат влијанието на промените во опкружувањето кон воведените заштитни сигурносни мерки, заради утврдување на потребата од воспоставување дополнителни мерки за намалување на ризиците.

    Заради намалување на ризиците, поврзани со влијанието на промените од став 1 на оваа точка, давателите на платежните услуги се должни да воспостават процес на управување со промените, со кој се обезбедува нивно соодветно планирање, тестирање и документирање, во согласност со доделените овластувања.

18. Давателите на платежните услуги се должни да воспостават принцип на поделба на должностите, преку раздвојување на информациските системи, односно системските околини за развој, тест и продукциско работење во делот на обезбедувањето на платежните услуги.

Мерки за обезбедување интегритет и доверливост на податоците и системите

19. Давателите на платежните услуги се должни да овозможат точност и релевантност на собирањето, преносот, обработката, чувањето, архивирањето и начинот на приказ на чувствителните податоци за плаќање на корисниците на платежните услуги, како и нивна ограниченост само на она што е неопходно за обезбедувањето на платежната услуга.

20. Давателите на платежните услуги се должни да извршуваат редовни проверки заради навремено спроведување на критичните сигурносни надградби на софтверот којшто се користи за обезбедување на платежните услуги, вклучително и на корисничкиот софтвер којшто е поврзан со плаќањето.

    Давателите на платежните услуги се должни да воспостават механизми за проверка на интегритетот на софтверот, вградените програми и информациите поврзани со платежните услуги.

Мерки за физичка заштита

21. Давателите на платежните услуги се должни да воспостават сигурносни мерки за физичка заштита на информациските системи и системите за комуникациска технологија коишто се употребуваат за обезбедување на платежните услуги, а заради заштита на чувствителните податоци за плаќањата.

Мерки за контрола на пристапот

22. Пристапот до информациските системи и системите за комуникациска технологија треба да им се овозможи само на овластените лица со оправдани деловни потреби. Овластувањата треба да се доделуваат во согласност со работните задачи на вработените, според принципот „неопходност од пристап".

    Давателите на платежните услуги се должни да воспостават надзор над пристапот и евиденција на активностите коишто се одвиваат на информациските системи и системите за комуникациска заштита.

23. Давателите на платежните услуги се должни да применуваат засилена контрола врз привилегираниот пристап до информациските системи и системите за комуникациска технологија, преку строго ограничување и подетален надзор над активностите со ваков пристап.

24. Евиденцијата во согласност со точка 22 став 2 од оваа одлука треба да се чува во период којшто одговара на критичноста на деловните функции, процесите за нивна поддршка и информативни средства, во согласност со точките 9 и 10 од оваа одлука.

    Давателите на платежните услуги информациите од став 1 од оваа точка се должни да ги користат за идентификација и спроведување истраги на невообичаени активности при давањето на платежните услуги.

25. Далечинскиот пристап до критичните информациски системи и системите за комуникациска технологија е одобрен во согласност со принципот „неопходност од пристап" и преку примена на засилена автентикација.

26. Функционирањето на продуктите, алатките и постапките поврзани со процесот на контрола на пристапот треба да бидат заштитени од нивно онеспособување или заобиколување.

Мерки за постојано следење и откривање

27. Давателите на платежните услуги се должни да воспостават процеси и функции за постојано следење на деловните функции, помошни процеси и информациски средства за нивна поддршка, заради навремено откривање на невообичаените активности при давањето на платежните услуги.

    Давателите на платежните услуги се должни да воспостават соодветни и ефективни функционалности за откривање физички и логички нарушувања на сигурноста коишто влијаат врз доверливоста, интегритетот и расположливоста на информациските средства коишто се употребуваат за платежните услуги.

28. Процесите на постојано следење и откривање треба да опфатат:
    - релевантни внатрешни и надворешни фактори, коишто ги вклучуваат деловните функции и функциите за администрација на информациските системи и системите за комуникација;
    - анализа на трансакциите којашто има за цел да обезбеди откривање злоупотреби на пристапот од страна на надворешни лица или други субјекти и
    - потенцијални внатрешни и надворешни закани.

29. Давателите на платежните услуги се должни да преземат мерки за откривање неавторизирано преземање информации, присуство на малициозен / злонамерен софтвер, присуство на ранливости во софтверот и хардверот и проверка за нови сигурносни надградби, како и останати сигурносни закани.

Мерки за оперативни или сигурносни инциденти

30. Давателите на платежните услуги се должни да воспостават соодветна организациска структура и ефективни процеси со кои се овозможува откривање, класификација, процена на значајноста, известување, следење и управување со оперативните или сигурносните инциденти.

31. Давателите на платежните услуги се должни да воспостават постапка за известување за оперативните или сигурносните инциденти и поплаки од корисниците на платежните услуги поврзани со сигурноста, до органот на управување.

    Давателот на платежните услуги е должен веднаш и без непотребно одлагање да ги информира своите корисници на платежните услуги за

инцидентот и за сите мерки коишто корисниците на платежните услуги можат да ги преземат за намалување на негативните ефекти на инцидентот.

Мерки за непрекинатост во работењето

32. Давателите на платежните услуги се должни да воспостават процеси за непрекинатост во работењето со што ќе се обезбеди непрекинатост при давањето на платежната услуга или минимизирање на загубите во случај на позначителен прекин во деловното работење.

33. Заради непрекинатоста во работењето, давателите на платежните услуги се должни да вршат квантитативна и квалитативна анализа на изложеноста кон поголеми прекини на работењето, за нивното потенцијално влијание со примена на анализа на внатрешни или надворешни податоци и анализа на применливи сценарија.

    Врз основа на утврдените критични функции, процеси, системи, нивната меѓусебна поврзаност и зависност, во согласност со точките 9, 10 и 11 од оваа одлука, давателите на платежните услуги се должни да им дадат приоритет на оние активности коишто произлегуваат од извршената процена на ризикот од обезбедување на непрекинатоста на работењето.

34. Врз основа на анализата, во согласност со точка 33 став 1 од оваа одлука, давателот на платежните услуги е должен да воспостави:
    - планови за непрекинатост на работењето заради преземање соодветна реакција при вонредни ситуации и обезбедување непрекинатост на своите критични деловни активности и
    - мерки коишто би се спровеле во случај на прекин на платежните услуги, за да се намали негативниот ефект врз платните системи и да им овозможи на корисниците на платежните услуги извршување на платежните трансакции коишто се во тек.

Планирање на непрекинатоста во работење преку анализа на применливи сценарија

35. Давателите на платежните услуги се должни да обработат различни, реални, вклучително и екстремни сценарија на коишто може да бидат изложени и да го проценат нивното потенцијално влијание врз непрекинатоста во работењето.

36. Во согласност со спроведената анализа од точка 33 став 1 од оваа одлука и сценаријата од точка 35 од оваа одлука, давателот на платежните услуги е должен да изработи планови за одговор и закрепнување коишто треба да се:
    - насочат кон обезбедување на функционалноста на критичните функции, процеси, системи и нивната меѓусебна зависност;
    - документирани и на располагање на организациските единици, како и да бидат лесно достапни во вонредни ситуации; и
    - редовно ажурирани во согласност со стекнатите искуства при тестирањето, утврдените нови ризици и закани, како и при промена на целите и приоритетите при закрепнувањето.

Тестирање на плановите за непрекинатоста во работењето

37. Давателите на платежните услуги се должни да ги тестираат своите планови за непрекинатост во работењето најмалку еднаш годишно.

    Со тестирањето наведено во став 1 на оваа точка, давателот на платежната услуга е должен да ја провери поддршката којашто ја нудат плановите за ефикасно воспоставување на целите за заштита, повторното воспоставување на интегритетот, расположливоста на деловните функции и доверливоста на информативните средства.

38. Плановите од точка 34, став 1, алинеја 1 се ажурираат најмалку еднаш годишно, во согласност со резултатите од спроведените тестирања, актуелните закани, новите сознанија и претходните искуства, промените во приоритети при обнова и закрепнување, како и врз база на анализата на применливи сценарија и по извршени промени во системи и процеси.

39. Тестирањето на плановите за непрекинатост на работењето на давателите на платежните услуги треба да:
    - вклучи соодветни применливи сценарија во согласност со точка 35 од оваа одлука;
    - е испланирано така, што ќе овозможи преиспитување на претпоставките врз кои се засноваат планови за непрекинатост на работењето, особено начинот на управување, одлучување и комуникација во вонредни ситуации и
    - вклучи постапки за проверка на обученоста на вработените и дефинираните постапки за соодветен одговор при наведените сценарија.

40. Давателите на платежните услуги се должни периодично да ја следат ефикасноста на своите планови за непрекинатост на работењето и да ги документираат и да ги анализираат сите утврдени проблеми или неуспешни тестови.

Мерки за комуникација во кризни ситуации

41. Давателите на платежните услуги, во случај на прекин на деловната активност или вонредна ситуација и при спроведување на плановите за непрекинатост во работењето, се должни да обезбедат ефикасни мерки за комуникација во кризни ситуации, за навремено и уредно информирање на сите релевантни засегнати страни, вклучително и надворешните лица кои извршуваат оперативни функции.

Тестирање на сигурносните мерки

42. Давателите на платежните услуги се должни да воспостават рамка за тестирање со која ќе се потврди ефективноста и ефикасноста на воспоставените сигурносни мерки. Рамката за тестирање треба да вклучува нови закани и слабости утврдени при следењето на ризиците.

43. Давателите на платежните услуги се должни во рамката од точка 42 од оваа одлука да вклучат, спроведување тестови, особено при значајни промени

во инфраструктурата, процеси или постапки и во случај на измени коишто се воведени како резултат на значајни оперативни или сигурносни инциденти.

44. Рамката за тестирање од точка 42 од оваа одлука треба да опфати тестирање на сигурносните мерки за:
    - платните терминали и уреди коишто се употребуваат при давањето на платежната услуга;
    - платните терминали и уреди коишто се употребуваат за автентикација на корисниците на платежните услуги и
    - уредите и софтверот за изработка и прием на кодот за автентикација ставени на располагање од давателот на платежните услуги на корисникот на платежните услуги.

45. Рамката за тестирање од точка 42 од оваа одлука, треба да обезбеди потврда за:
    - спроведување на постапката, дел од формалниот процес на управување со промените кај давателот на платежните услуги, за потврда на ефективноста и ефикасноста на воведените мерки;
    - спроведување објективно тестирање од лица со потребно знаење, вештини и стручност при тестирањето на воведените сигурносни мерки во платежните услуги и независност на лицата при што тие не биле вклучени при развивањето на сигурносните мерки за платежните услуги коишто се тестираат и
    - вклученост во тестирањето на постапките за проверка на постоењето на ранливости и тестирање на отпорноста на системите коишто се соодветни за утврденото ниво на ризик во однос на платежните услуги коишто се даваат.

46. Давателите на платежните услуги се должни да спроведуваат тестирања на сигурносните мерки за своите платежните услуги во согласност со следната фреквенција:
    - за системите коишто не се критични, фреквенцијата на тестирање зависи од проценатa на ризиците, но тие треба да се тестираат најмалку еднаш на секои три години,
    - за системите коишто се критични за обезбедување на нивните платежни услуги, како што е наведено во регистарот од точка 10 од оваа одлука, тестирањето на сигурносните мерки треба да се спроведува најмалку еднаш годишно.

47. Давателите на платежните услуги се должни да ги следат и да ги анализираат резултатите од спроведените тестирања и во согласност со нив, да ги ажурираат своите сигурносни заштитни мерки.

    Во случај на утврдени слабости при тестирањето на сигурносните мерки на системите коишто се утврдени како критични во согласност со точка 10, давателите на платежните услуги се должни ажурирањето на сигурносните мерки да го направат без непотребно одлагање.

Подигање на свесноста и постојана обука

48. Давателите на платежните услуги должни да воспостават и да воведат процеси и организациска структура за утврдување и постојано следење на сигурносните и оперативните закани коишто може значително да влијаат врз давањето на платежните услуги.

49. Давателите на платежните услуги се должни врз база на извршените анализи на утврдените или настанатите оперативни или сигурносни инциденти, кај давателот или надвор од давателот соодветно да ги ажурираат сигурносните мерки.

50. Давателите на платежните услуги се должни да изработат и спроведат план за обука на сите вработени којашто ќе овозможи извршување на нивните работни задачи во согласност со политиката за сигурност и постапките коишто имаат цел да придонесат за намалување на можностите од човечка грешка, кражба, измама, злоупотреба или загуба.

    Во согласност со планот од став 1 на оваа точка, давателите на платежните услуги се должни да обезбедат обука на вработените најмалку еднаш годишно, а доколку е потребно и почесто.

51. Давателите на платежните услуги се должни да им овозможат на вработените коишто извршуваат клучни улоги, утврдени во согласност со точка 9 од оваа одлука, специјализирана обука за информациска сигурност најмалку еднаш годишно или почесто, доколку е потребно.

Поддршка и информирање на корисниците на платежните услуги

52. Давателите на платежните услуги се должни да воспостават постапка за ефективна поддршка на корисниците на платежните услуги, за сите нивни прашања и барања, известувања за невообичаени појави и проблеми поврзани со сигурноста на платежните услуги, заради подигнување на свесноста за сигурносните ризици при извршувањето на платежните услуги.

    Давателот на платежната услуга е должен да ги информира корисниците на платежните услуги за начинот на кој ќе ја овозможи потребната поддршка.

53. Давателот на платежните услуги е должен да му овозможи на корисникот на платежните услуги да го оневозможи користењето на одредени функционалности коишто се поврзани со платежните услуги, а се ставени на располагање на корисникот.

54. Давателот на платежните услуги, којшто се договорил со плаќачот за ограничување на потрошениот износ на платежните трансакции коишто се извршуваат преку одреден платен инструмент, е должен да му овозможи на плаќачот приспособување на тие ограничувања до износот на највисокото договорено ограничување.

55. Давателите на платежните услуги се должни да ги предупредат корисниците на платежните услуги за иницирање или неуспешни обиди за

иницирање платежни трансакции, заради откривање сомнеж за измамничко или злонамерно користење со нивните платежни сметки.

56. Давателите на платежните услуги се должни да ги информираат корисниците на платежните услуги за ажурирањата на сигурносните мерки и постапки коишто влијаат врз корисниците при давањето на платежните услуги.

IV. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

57. Давателите на платежните услуги се должни да го усогласат своето работење со барањата на оваа одлука најдоцна до 19 февруари 2024 година.

    Давателите на платежните услуги коишто се основани до денот на започнување на примена на оваа одлука и коишто имаат дозвола за основање и работење на банка се должни соодветно да го усогласат постојниот систем за управување со оперативниот ризик воспоставен во согласност со Одлуката за методологијата за управување со ризиците на банката („Службен весник на Република Македонија" бр. 113/19, 69/20 и 314/20), со одредбите од оваа одлука.

58. Оваа одлука влегува во сила на денот на објавувањето во „Службен весник на Република Северна Македонија".

О бр.02-15/XXII-8/2022
28 декември 2022 година
Скопје

Гувернер и
претседавач на
Советот на Народна банка на
Република Северна Македонија
Д-р Анита Ангеловска-Бежоска