На основу члана 15. став 1. и члана 63. став 2. Закона о Народној банци Србије („Службени гласник РС“, бр. 72/2003, 55/2004, 85/2005 – др. закон, 44/2010, 76/2012, 106/2012, 14/2015 и 40/2015 – одлука УС), Извршни одбор Народне банке Србије доноси

О Д Л У К У
О ИЗМЕНАМА И ДОПУНАМА ОДЛУКЕ О МИНИМАЛНИМ СТАНДАРДИМА УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМОМ ФИНАНСИЈСКЕ ИНСТИТУЦИЈЕ

1. У Одлуци о минималним стандардима управљања информационим системом финансијске институције („Службени гласник РС“, бр. 23/2013 и 113/2013) (у даљем тексту: Одлука), у тачки 1, став 1. мења се и гласи:

„Овом одлуком утврђују се минимални стандарди и услови стабилног и сигурног пословања који се односе на управљање информационим системима у банкама, друштвима за осигурање, даваоцима финансијског лизинга, друштвима за управљање добровољним пензијским фондовима, као и платним институцијама, институцијама електронског новца и јавном поштанском оператору у делу њиховог пословања који се односи на пружање платних услуга и/или издавање електронског новца (у даљем тексту: финансијска институција).“.

2. У тачки 2, одредба под 35), речи: „пре наступања нерасположивости пословног процеса који не би био обухваћен резервном копијом података“ замењују се речима: „од последње резервне копије података до наступања нерасположивости пословног процеса“.

Одредба под 37) мења се и гласи:

„37) *електронске услуге* су услуге које клијенти банке, платне институције, институције електронског новца и јавног поштанског оператора користе са удаљене локације преко интернета, а које обухватају приступање платном и другом рачуну, иницирање платне трансакције и друге активности којима се приступа подацима у вези са услугама ових финансијских институција који би могли бити предмет преварних радњи или других злоупотреба.“.

3. У тачки 22, после става 1, додаје се став 2, који гласи:

„Финансијска институција је нарочито дужна да обезбеди интегритет података о платним трансакцијама при њиховој обради, чувању и предузимању свих других радњи у вези с тим подацима.“.

4. У тачки 26, ст. 1. и 7, речи: „и друштва за управљање добровољним пензијским фондом“ замењују се речима: „,друштва за управљање добровољним пензијским фондом, платне институције, институције електронског новца и јавног поштанског оператора“.

5. У тачки 42, став 1, одредба под 3), тачка на крају реченице замењује се запетом и додају се речи: „која мора да садржи списак мера и активности које је потребно предузети, као и динамику њиховог спровођења од тренутка престанка пружања уговорених услуга до избора другог пружаоца услуга или потпуног успостављања процеса обављања тих активности унутар финансијске институције.“.

6. У тачки 44, после става 1, додаје се нови став 2, који гласи:

„Финансијска институција је дужна да обезбеди да пружалац услуга поверене активности обавља у складу са политиком безбедности информационог система и другим актима финансијске институције којима се уређује безбедност њеног информационог система.“.

Досадашњи став 2. постаје став 3.

7. У тачки 45, после става 1, додаје се нови став 2, који гласи:

„Ако се мења уговор из става 1. ове тачке, а да се при том не мења поверена активност, пружалац услуга или се не утиче на резултате анализе из тачке 42. став 1. одредба под 1) ове одлуке, односно на резултате процене из тачке 42. став 2. те одлуке, финансијска институција је дужна да пре закључења тог уговора о томе обавести Народну банку Србије и достави јој нацрт уговора.“.

Досадашњи став 2. постаје став 3.

8. Тач. 49. до 51, као и наслов изнад тих тачака, мењају се и гласе:

„IX. ЕЛЕКТРОНСКЕ УСЛУГЕ

49. Банка, платна институција, институција електронског новца и јавни поштански оператор који пружају електронске услуге (у даљем тексту: пружалац електронских услуга) дужни су да, као саставни део управљања ризиком информационог система, успоставе процес управљања ризицима који произлазе из пружања електронских услуга.

50. Пружалац електронских услуга дужан је да при пружању електронских услуга примени безбедне и ефикасне методе за проверу и потврду идентитета и овлашћења лица, процеса и система.

Пружалац електронских услуга дужан је да корисницима при коришћењу ових услуга обезбеди аутентификацију која укључује комбинацију најмање два међусобно независна елемента за потврђивање корисничког идентитета.

Изузетно од става 2. ове тачке, пружалац електронских услуга може применити аутентификацију корисника која се врши коришћењем једног елемента за потврђивање корисничког идентитета, у случају:

1) плаћања мале новчане вредности, у складу са оквирним уговором о платним услугама, под условом да се ризицима који се односе на укупан износ ових плаћања управља на одговарајући начин (нпр. утврђивање максималног износа ових трансакција у одређеном периоду након којих ће се спровести аутентификација у складу са ставом 2. ове тачке или предузети додатне мере заштите),

2) плаћања према примаоцима плаћања која је платилац унапред одредио (нпр. утврђивање тзв. беле листе примаоца плаћања),

3) пренос новчаних средстава између два платна рачуна истог корисника код истог пружаоца електронских услуга,

4) пренос електронског новца који се обавља у оквиру истог пружаоца електронских услуга, који је заснован на анализи ризика ових платних трансакција,

5) других трансакција и услуга које су на основу анализе ризика процењене као нискоризичне.

Пружалац електронских услуга може да примени аутентификацију корисника из става 3. ове тачке само ако је најмање 30 дана пре дана почетка пружања услуге о томе обавестио Народну банку Србије и уз то обавештење доставио свеобухватну и детаљну анализу ризика и начина управљања ризицима који произлазе из

пружања услуга на начин утврђен у одредбама 1) до 5) тог става и другу одговарајућу документацију која се односи на ову анализу.

Анализа из става 4. ове тачке обухвата посебно и анализе из става 3. одредбе под 4) и 5) ове тачке, ако пружалац електронских услуга намерава да примени аутентификацију корисника коришћењем једног елемента за потврђивање корисничког идентитета у случајевима из тих одредаба.

Рок из става 4. ове тачке рачуна се од дана достављања уредне документације из тог става.

51. Пружалац електронских услуга дужан је да усвоји и примени правила којима се на одговарајући начин, у складу с тржишном праксом и проценом ризика, ограничава број покушаја пријаве на систем за пружање електронских услуга, односно покушаја аутентификације, да одреди најдуже време без активности корисника након пријаве на тај систем, као и да утврди рокове важења параметара аутентификације.

При коришћењу једнократних лозинки ради аутентификације (нпр. *One Time Password – OTP*), пружалац електронских услуга дужан је да обезбеди да временско важење те лозинке буде ограничено на период који је потребан за обављање аутентификације.

Пружалац електронских услуга дужан је да утврди највећи могући број неуспешних покушаја пријаве на систем за пружање електронских услуга након којих ће тај систем бити трајно или привремено блокиран, као и да успостави процедуре за безбедно поновно активирање овог система.

Пружалац електронских услуга дужан је да утврди најдуже могуће време без активности корисника на систему за пружање електронских услуга по пријављивању у тај систем, након којег долази до аутоматског одјављивања корисника из овог система (тзв. завршетак сесије).

Пружалац електронских услуга дужан је да обезбеди одговарајућу потврду свог идентитета на дистрибутивном каналу за пружање електронских услуга како би корисници могли да провере пружаоца електронске услуге.

Пружалац електронских услуга је дужан да обезбеди постојање оперативних и системских записа како би се у одговарајућој мери

обезбедила непорецивост и доказивост радњи у вези са пружањем електронских услуга.“.

9. Банке су дужне да своје пословање ускладе са одредбама ове одлуке до дана почетка њене примене.

Јавни поштански оператор је дужан да своје пословање усклади са одредбама Одлуке и ове одлуке до 1. јула 2017. године, осим тачке 2. став 2. и тачке 8. ове одлуке са којима је дужан да то пословање усклади до дана почетка њене примене.

10. Ова одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику РС“, а примењује се од 1. априла 2017. године.

ИО НБС бр. 1
12. јануара 2017. године
Б е о г р а д

Председавајућа
Извршног одбора Народне банке Србије
Г у в е р н е р
Народне банке Србије

др Јоргованка Табаковић, с.р.