EBA/GL/2017/17

12/01/2018

Насоки

относно мерките за сигурност за операционните рискове и рисковете, свързани със сигурността, за платежните услуги съгласно Директива (ЕС) 2015/2366 (Втора директива за платежните услуги)

1. Спазване на насоките задълженията за докладване

Status of these guidelines

1. Този документ съдържа насоки, издадени съгласно член 16 от Регламент (ЕС) № 1093/2010 . Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010, компетентните органи и финансовите институции полагат всички усилия за спазване на насоките.

2. В насоките е представено становището на ЕБО за подходящите надзорни практики в Европейската система за финансов надзор или за това как правото на Съюза следва да се прилага в дадена област. Компетентните органи, както са дефинирани в член 4, параграф 2 от Регламент (ЕС) № 1093/2010, за които се отнасят тези насоки, трябва да ги спазват, като ги включат в практиките си по подходящ начин (напр. като изменят своята правна рамка или надзорни процеси), включително когато насоките са насочени основно към институциите.

Изисквания за отчетност

3. Съгласно член 16, параграф 3 от Регламент (ЕС) № 1093/2010, най-късно до 12.03.2018 компетентните органи са длъжни да уведомят ЕБО дали спазват или възнамеряват да спазват тези насоки, в противен случай - за причините за неспазване. При липса на уведомление в този срок ЕБО счита, че компетентните органи не спазват изискването за отчетност. Уведомленията трябва да се изпратят чрез подаване на формата, намираща се на уебсайта на ЕБО, на адрес compliance@eba.europa.eu, като се посочи референтен номер 'EBA/GL/2017/17"'. Уведомленията следва да се подават от лица, оправомощени да докладват за наличието на съответствие от името на техните компетентни органи. Всяка промяна в статута на спазването трябва също да се отчита пред ЕБО.

4. Уведомленията се публикуват на уебсайта на ЕБО в съответствие с член 16, параграф 3.

2. Предмет, обхват и определения

Предмет и обхват

5. Настоящите насоки изпълняват мандат, предоставен на ЕБО съгласно член 95, параграф 3 от Директива (ЕС) № 2015/2366[1] (Втора директива за платежните услуги).

6. Настоящите насоки определят изискванията за установяването, прилагането и наблюдението на мерките за сигурност, които ДПУ трябва да предприемат, в съответствие с член 95, параграф 1 от Директива (ЕС) 2015/2366, за управление на операционните рискове и рисковете, свързани със сигурността, във връзка с платежните услуги, които предоставят.

Адресати

7. Настоящите насоки са предназначени за ДПУ, както са определени в член 4, параграф 11 на Директива (ЕС) 2015/2366 и както е посочено в определението за "финансови институции" в член 4, параграф 1 от Регламент (ЕС) 1093/2010, и за компетентните органи, както са определени в член 4, параграф 2, подточка i) от същия Регламент посредством препратка към отменената Директива 2007/64/ЕО[2] (по настоящем Директива (ЕС) 2015/2366[3]).

Определения

8. Освен ако не е посочено друго, термините, използвани и определени в Директива (ЕС) 2015/2366, имат същото значение в настоящите насоки. В допълнение за целите на настоящите насоки се прилагат следните определения:

Ръководен орган	–	За ДПУ, които са кредитни институции, този термин има същото значение като определението в член 3, параграф 1, точка 7 на Директива 2013/36/ЕС[4];

[1] Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 Ноември 2015 г. за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО (ОВ L 337, 23.12.2015 г., стр. 35)

[2] Директива 2007/64/ЕО на Европейския парламент и на Съвета от 13 Ноември 2007 г. относно платежните услуги във вътрешния пазар, за изменение на директиви 97/7/ЕО, 2002/65/ЕО, 2005/60/ЕО и 2006/48/ЕО и за отмяна на Директива 97/5/ЕО (ОВ L 319, 5.12.2007 г.).

[3] В съответствие с член 114, втори подпараграф от Директива (ЕС) 2015/2366, всички позовавания към отменената Директива 2007/64/ЕО следва да се разбират като позовавания към Директива (ЕС) 2015/2366 и се четат в съответствие с таблицата на съответствието в Приложение II към Директива (ЕС) 2015/2366.

[4] Директива 2013/36/ЕС на Европейския парламент и на Съвета относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници, за изменение на Директива 2002/87/ЕО и за отмяна на директиви 2006/48/ЕО и 2006/49/ЕО, (ОВ L 176, 27.6.2013 г., стр. 338).

	– За ДПУ, които са платежни институции или институции за електронни пари, този термин означава директори или лица, отговарящи за управлението на ДПУ, и, където е приложимо, лица, отговарящи за управлението на дейността по предоставяне на платежни услуги на ДПУ; – За ДПУ, посочени в член 1, параграф 1, точки в), д) и е) от Директива (ЕС) 2015/2366, този термин има значението, което е определено от приложимото законодателство на ЕС или националното законодателство.
Операционен или свързан със сигурността инцидент	Единично събитие или поредица от свързани събития, които не са планирани от доставчика на платежни услуги и които имат или вероятно ще окажат неблагоприятно въздействие върху целостта, достъпността, поверителността, автентичността и/или непрекъснатостта на свързаните с плащания услуги.
Висше ръководство	(а) За ДПУ, които са кредитни институции, този термин има същото значение като определението в член 3, параграф 1, точка 9 на Директива 2013/36/ЕС; (б) За ДПУ, които са платежни институции или институции за електронни пари, този термин означава физически лица, които упражняват изпълнителни функции в институцията и които са отговорни и подотчетни на ръководния орган за ежедневното управление на ДПУ; (в) За ДПУ, посочени в член 1, параграф 1, точки в), д) и е) от Директива (ЕС) 2015/2366, този термин има значението, което е определено от приложимото законодателство на ЕС или националното законодателство.
Риск за сигурността	Риск, произтичащ от неподходящи или неуспешни вътрешни процеси или външни събития, които имат или вероятно ще окажат неблагоприятно въздействие върху достъпността, целостта, поверителността на системите за информационни и комуникационни технологии и/или информацията, използвана за предоставянето на платежни услуги. Това включва риска от кибератаки или неподходящи мерки за физическа сигурност.
Склонност към поемане на риск	Съвкупното равнище и видовете рискове, които институцията е готова да поеме в рамките на своя капацитет за поемане на риск, в съответствие със своя бизнес модел за постигнене на стратегическите си цели.

3. Въвеждане

Дата на прилагане

9. Настоящите насоки се прилагат от 13 януари 2018 г.

4. Насоки

Насока 1: Общ принцип

1.1 Всички ДПУ следва да спазват всички разпоредби, определени в насоките. Нивото на детайлност следва да бъде пропорционално на размера на ДПУ, както и на естеството, обхвата, сложността и рисковете, свързани с конкретните услуги, която ДПУ предоставя или възнамерява да предоставя.

Насока 2: Вътрешно управление

Рамка за управление на операционния риск и риска за сигурността

2.1 Доставчиците на платежни услуги следва да въведат ефективна рамка за управление на операционния риск и на риска, свързан със сигурността (по-долу "рамка за управление на риска"), която следва да подлежи на одобрение и преразглеждане поне веднъж годишно от страна на ръководния орган и, където е приложимо, от висшето ръководство. Тази рамка следва да поставя акцент върху мерките за сигурност за намаляване на операционните рискове и рисковете, свързани със сигурността и следва да бъде изцяло внедрена в цялостните процеси за управление на риска на ДПУ.

2.2 Рамката за управление на риска следва:

а) да включва изчерпателен документ относно политиката по сигурността, както е определено в член 5, параграф 1, буква й) от Директива (ЕС) 2015/2366;

б) да съответства на склонността към поемане на риск на ДПУ;

в) да определя и да възлага ключови роли и отговорности, включително и линиите за докладване, необходими за налагане на мерките за сигурност и за управление на рисковете за сигурността и операционните рискове;

г) да въведе необходимите процедури и системи за идентифициране, измерване, наблюдение и управление на различните рискове, произтичащи от свързаните с плащания дейности на ДПУ и на които ДПУ е изложен, включително правила за осигуряване на непрекъснатост на дейността.

2.3 Доставчиците на платежни услуги следва да гарантират, че рамката за управление на риска е надлежно документирана и обновявана с документиран натрупан опит в хода на нейното изпълнение и наблюдение.

2.4 Доставчиците на платежни услуги следва да гарантират, че преди всяко голямо изменение на инфраструктурата, процесите или процедурите и след всеки голям операционен инцидент или инцидент, свързан със сигурността на платежните услуги, които предоставят,

ДПУ следва да извършват преглед на необходимостта от промени или подобрения на рамката за управление на риска, без неоснователно забавяне.

Управление на риска и модели за контрол

2.5 Доставчиците на платежни услуги следва да въведат три ефективни линии на защита или еквивалентен вътрешен модел за управление и контрол на риска за идентифициране и управление на операционните рискове и рисковете, свързани със сигурността. Доставчиците на платежни услуги следва да гарантират, че гореспоменатият модел за вътрешен контрол разполага с достатъчни правомощия, независимост, ресурси и линии за пряко докладване към ръководния орган и, ако е приложимо, към висшето ръководство.

2.6 Мерките за сигурност, определени в настоящите насоки следва да бъдат одитирани от одитори с експертни познания в областта на ИТ сигурността и плащанията и които са операционно независими в рамките на или от ДПУ. При определяне честотата и акцента на такива одити следва да се вземат предвид съответните рискове, свързани със сигурността.

Възлагане на дейности на външни изпълнители

2.7 Доставчиците на платежни услуги следва да гарантират ефективността на мерките за сигурност, определени в настоящите насоки, когато оперативните функции на платежните услуги, включително ИТ системите, се възлагат на външни изпълнители.

2.8 Доставчиците на платежни услуги следва да гарантират, че в договорите и споразуменията на ниво услуги с доставчиците, на които възлагат функции, са заложени подходящи и професионални цели, свързани със сигурността. Доставчиците на платежни услуги следва да наблюдават и да търсят потвърждение за нивото на съответствие на тези доставчици с целите, мерките и очакваните резултати по отношение на сигурността.

Насока 3: Оценка на риска

Определяне на функциите, процесите и активите

3.1 Доставчиците на платежни услуги следва да определят, въведат и редовно да обновяват списък със своите бизнес функции, ключови роли и помощни процеси, за да установят важността на всяка функция, роля и помощен процес, както и техните взаимозависимости по отношение на операционните рискове и рисковете, свързани със сигурността.

3.2 Доставчиците на платежни услуги следва да определят, въведат и редовно да обновяват списък с информационните активи, като системи за информационни и комуникационни технологии, техните конфигурации, други инфраструктури, както и взаимозависимостите с други вътрешни и външни системи, за да могат да управляват активите, които поддържат техните критични бизнес функции и процеси.

Класификация на функциите, процесите и активите

3.3 Доставчиците на платежни услуги следва да класифицират определените стопански функции, помощни процеси и информационни активи по отношение на тяхната критичност.

Оценка на риска по отношение на функциите, процесите и активите

3.4 Доставчиците на платежни услуги следва да гарантират, че наблюдават непрекъснато заплахите и уязвимостта и редовно преглеждат рисковите сценарии, които могат да окажат влияние на техните бизнес функции, критични процеси и информационни активи. Като част от задължението си да извършват и предоставят на компетентните органи обновена и цялостна оценка на операционните и рисковете, свързани със сигурността, свързани с платежните услуги, които предоставят и относно адекватността на мерките за намаляване и контролните механизми, въведени в отговор на тези рискове, както е заложено в член 95, параграф 2 от Директива (ЕС) 2015/2366, ДПУ следва да извършват и документират оценките на риска най-малко веднъж годишно или на по-кратки интервали, установени от компетентните органи, на функциите, процесите и информационните активи, които са определили и класифицирали, за да определят и оценят ключовите операционни рискове и рисковете, свързани със сигурността. Такива оценки на риска следва също да бъдат извършвани преди всяка голяма промяна на инфраструктурата, процесите и процедурите, оказваща въздействие върху сигурността на платежните услуги.

3.5 На основата на оценките на риска ДПУ следва да определят дали и до каква степен може да са необходими промени на съществуващите мерки за сигурност, използваните технологии и процедури или на предлаганите платежни услуги. Доставчиците на платежни услуги следва да вземат предвид времето, необходимо за въвеждане на промените, и времето за въвеждане на подходящи временни мерки за сигурност за минимизиране на риска от операционни инциденти или инциденти, свързани със сигурността, измами и потенциалното неблагоприятно въздействие върху предоставянето на платежни услуги.

Насока 4: Защита

4.1 Доставчиците на платежни услуги следва да установят и въведат превантивни мерки за сигурност срещу установените операционни рискове и рисковете, свързани със сигурността. Тези мерки следва да гарантират подходящо ниво на сигурност в съответствие с установените рискове.

4.2 Доставчиците на платежни услуги следва да установят и следват подход на „защита в дълбочина“ като въведат многослойни контролни механизми, обхващащи хора, процеси и технологии, като всяко ниво трябва да служи като спасителна мрежа за предходните нива. „Защитата в дълбочина“ следва да се разбира като такава с определени няколко контролни механизми, обхващащи един и същ риск, като например принципа на четирите очи,

двуфакторно удостоверяване на идентичността, сегментация на мрежата и множество защитни стени.

4.3 Доставчиците на платежни услуги следва да гарантират поверителността, целостта и достъпността на своите критични логически и физически активи, ресурси и чувствителни данни за плащанията на своите ППУ при тяхното съхранение, пренос и употреба. Ако данните включват лични данни, такива мерки следва да бъдат въведени в съответствие с Регламент (ЕС) 2016/679[5] или, ако е приложимо, Регламент (ЕС) 45/2001.[6]

4.4 Доставчиците на платежни услуги следва да следят непрекъснато дали промените на съществуващата оперативна среда влияят на съществуващите мерки за сигурност и дали налагат предприемането на допълнителни мерки за смекчаване на свързаните рискове. Тези промени следва да са предмет на формалния процес на ДПУ за управление на промените, който следва да гарантира, че промените са надлежно планирани, тествани, документирани и одобрени. На основата на наблюдаваните заплахи за сигурността и извършените промени следва да бъде извършвано тестване, за да бъдат включени сценарии за актуалните и познатите потенциални атаки.

4.5 При проектирането, разработването и предоставянето на платежни услуги, ДПУ следва да гарантират, че се прилагат принципите на сегрегация на задълженията и на „най-малко привилегии“. Доставчиците на платежни услуги следва да обръщат специално внимание на сегрегацията на ИТ средите в частност на средите за разработване, тестване и производство.

Цялост и поверителност на данните и системите

4.6 При проектирането, разработването и предоставянето на платежни услуги ДПУ следва да гарантират, че събирането, препращането, обработката, съхранението и/или архивирането и визуализацията на чувствителни данни за плащания на ППУ са адекватни, актуални и се ограничават до необходимото за предоставянето на платежните услуги.

4.7 Доставчиците на платежни услуги следва редовно да проверяват дали използваният софтуер за предоставяне на платежни услуги, включително софтуерът за плащания на потребителите, са актуални и се въвеждат значими за сигурността подобрения (пачове). Доставчиците на платежни услуги следва да гарантират, че са въведени механизми за проверка на целостта с цел удостоверяване целостта на софтуера, фърмуера и информацията за техните платежни услуги.

[5] Регламент (ЕС) на Европейския парламент и на Съвета от 27 Април 2016 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на личните данни) (ОВ L 119, 4.5.2016 г., стр. 1).

[6] Регламент (ЕС) 45/2001 на Европейския парламент и на Съвета от 18 Декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1).

Физическа сигурност

4.8 Доставчиците на платежни услуги следва да разполагат с въведени подходящи мерки за физическа сигурност в частност за защита на чувствителни данни за плащанията на ППУ, както и на системата за информационни и комуникационни технологии, използвани за предоставянето на платежни услуги.

Контрол на достъпа

4.9 Физическият и логическият достъп до системите за информационни и комуникационни технологии следва да бъде позволен единствено на оправомощени лица. Оправомощаването следва да бъде предоставяно според задачите и отговорностите на персонала и да се ограничава до лица, които са подходящо обучени и наблюдавани. Доставчиците на платежни услуги следва да въведат контролни механизми, които да ограничават по надежден начин такъв достъп до системите за информационни и комуникационни технологии до лицата с легитимно бизнес изискване. Електронният достъп на приложенията до данните и системите следва да бъде ограничен до минимумът, който се изисква за предоставянето на съответната услуга.

4.10 Доставчиците на платежни услуги следва да въведат строги контролни механизми върху привилегирования достъп до системата, като стриктно ограничават и наблюдават отблизо персонала със завишени права на достъп до системите. Следва да бъдат въведени контролни механизми като достъп и вход на основата на ролята, записване (регистриране) и преглед на системните дейности на потребителите с привилегии, надеждно удостоверяване на идентичността и следене за нередности. Доставчиците на платежни услуги следа да управляват правилата за достъп до информационните активи и техните помощни системи на основата на принципа "необходимост да се знае". Правата за достъп следва да бъдат преразглеждани периодично.

4.11 Регистрите на достъпа следва да бъдат пазени за период, който е съизмерим с критичното значение на определените бизнес функции, помощни процеси и информационни активи в съответствие с насока 3.1 и насока 3.2 без да се засягат изискванията за запазване, определени в законодателството на ЕС и националното законодателство. Доставчиците на платежни услуги следва да използват тази информация за улесняване на процеса на установяване и разследване на неправомерни действия, които са били открити при предоставянето на платежните услуги.

4.12 За да се гарантира сигурността на комуникациите и да се намали риска, дистанционен административен достъп до критични компоненти на информационните и комуникационните технологии следва да се предоставя само на принципа "необходимост да се знае" и когато се използват надеждни решения за удостоверяване на идентичността.

4.13 Функционирането на продуктите, инструментите и процедурите, свързани с процесите за контрол на достъпа следва да гарантират, че процесите за контрол на достъпа не са

засегнати или заобиколени. Това включва въвеждане, доставка, отмяна и изтегляне на съответните продукти, инструменти и процедури.

Насока 5: Откриване

Постоянно наблюдение и откриване

5.1 Доставчиците на платежни услуги следва да установят и въведат процеси и функции за постоянно наблюдение на бизнес функциите, помощните процеси и информационните активи за откриването на неправомерни действия в предоставянето на платежните услуги. Като част от постоянното наблюдение ДПУ следва да са въвели подходящи и ефективни механизми за откриване на физическо или логическо вмешателство, както и нарушаване на поверителността, целостта и достъпността на информационните активи, използвани за предоставянето на платежните услуги.

5.2 Процесите за постоянно наблюдение и откриване следва да обхващат:

а) съответните вътрешни и външни фактори, включително бизнес функциите и административните функции, свързани с информационните и комуникационните технологии;

б) трансакциите с цел откриване на злоупотреби с достъпа от страна на доставчици на услуги или други лица; и

в) потенциалните вътрешни и външни заплахи.

5.3 Доставчиците на платежни услуги следва да въведат мерки за откриване с цел установяване на потенциални изтичания на информация, зловреден код и други заплахи за сигурността, както и обществено известни уязвимости за софтуера и хардуера и проверка за съответните обновления относно сигурността.

Наблюдение и отчитане на операционни инциденти или инциденти, свързани със сигурността

5.4 Доставчиците на платежни услуги следва да определят подходящи критерии и прагове за класифициране на събитие като операционен инцидент или инцидент, свързан със сигурността, както е определено в раздел "Определения" от настоящите насоки, както и индикатори за ранно предупреждение, служещи за известяване, което да позволи на ДПУ ранно откриване на операционните инциденти и инцидентите, свързани със сигурността.

5.5 Доставчиците на платежни услуги следва да въведат подходящи процеси и организационни структури, за да гарантират последователно и цялостно наблюдение, обработка и предприемане на последващи действия за операционните инциденти и инцидентите, свързани със сигурността.

5.6 Доставчиците на платежни услуги следва да въведат процедура за отчитане до висшето ръководство на такива операционни рискове и рискове, свързани със сигурността, както и на клиентски оплаквания, свързани със сигурността.

Насока 6: Непрекъснатост на дейността

6.1 Доставчиците на платежни услуги следва да изготвят надежден план за управление на непрекъснатостта на дейността, който да гарантира тяхната способност за постоянно предоставяне на платежни услуги и да ограничава загубите в случай на сериозно смущение на дейността.

6.2 С цел да създаде надежден план за управление на непрекъснатостта на дейността, ДПУ следва да анализират внимателно до каква степен са изложени на сериозни смущения и да оценят (количествено и качествено) тяхното потенциално въздействие, използвайки вътрешни и/или външни данни и сценариен анализ. На основата на определените и класифицирани критични функции, процеси, системи, трансакции и взаимозависимости в съответствие с насоки 3.1 - 3.3 ДПУ следва да дадат приоритет на действията за осигуряване на непрекъснатостта на дейността, като използват подход, базиран на риска, който може да се основава на оценките на риска, извършени съгласно насока 3. В зависимост от бизнес модела на ДПУ това може, например, да улесни по-нататъшната обработка на критичните трансакции, докато продължават усилията за възстановяване.

6.3 На основата на анализа, извършен съгласно насока 6.2, ДПУ следва да въведат:

а) планове за непрекъснатост на дейността, които да гарантират, че могат да реагират адекватно при извънредни случаи и че имат възможност да поддържат критичните бизнес дейности; и

б) мерки за смекчаване, които да бъдат приети в случай на прекъсване на платежните услуги и прекратяване на съществуващите договори, за да бъде избегнато неблагоприятното въздействие върху платежните системи и върху ППУ и за да се гарантира осъществяването на неизпълнените платежни трансакции.

Планиране на непрекъснатостта на дейността на основата на сценарии

6.4 Доставчиците на платежни услуги следва да разгледат набор от различни сценарии, на които могат да бъдат изложени, включително екстремни, но реалистични такива и да оценят потенциалното им въздействие.

6.5 На основата на анализа, извършен съгласно насока 6.2 и реалистичните сценарии, определени съгласно насока 6.4, ДПУ следва да разработят планове за реакция и възстановяване, които следва:

а) да поставят акцент на въздействието върху дейността на критичните функции, процеси, системи, трансакции и взаимозависимости;

б) да бъдат документирани и предоставени на търговските и помощните отдели и леснодостъпни в извънредни случаи;

в) да бъдат обновявани в съответствие с натрупания опит от тестовете, установените нови рискове и заплахи и променените цели и приоритети за възстановяване.

Тестване на плановете за непрекъснатост на дейността

6.6 Доставчиците на платежни услуги следва да тестват своите планове за непрекъснатост на дейността и да гарантират, че действието на критичните функции, процеси, системи, трансакции и взаимозависимости се тества поне веднъж годишно. Плановете следва да подпомагат целите за защита и, ако е необходимо, възстановяване на целостта и достъпността на техните операции, както и поверителността на техните информационни активи.

6.7 Плановете следва да бъдат обновявани поне веднъж годишно на основата на резултатите от тестовете, текущите данни за заплахите, обмена на информация, натрупания опит от предишни събития, променените цели за възстановяване, както и анализ на оперативни и технически реалистични сценарии, които още не са се случвали, и, ако е приложимо, след промени в системата и процесите. Доставчиците на платежни услуги следва да се консултират и да съгласуват със съответните вътрешни и външни заинтересовани страни по време на въвеждането на своите планове за непрекъснатост на дейността.

6.8 Тестването от страна на ДПУ на техните планове за непрекъснатост на дейността следва:

а) да включва адекватен набор от сценарии, както е посочено в насока 6.4;

б) да бъде проектирано, така че да изпитва предположенията, на които се основават плановете, включително правилата за управление и плановете за комуникация при извънредни ситуации; и

в) да включва процедури за потвърждаване на способността на персонала и на процесите за адекватна реакция в горните сценарии.

6.9 Доставчиците на платежни услуги следва периодично да проверяват ефективността на своите планове за непрекъснатост на дейността и да документират и анализират всички предизвикателства или неуспехи в резултатите от тестовете.

Комуникация при извънредни ситуации

6.10 В случай на смущение или извънредна ситуация и при изпълнението на плановете за непрекъснатост на дейността ДПУ следва да гарантират, че разполагат с въведени ефективни мерки за комуникация при извънредни ситуации, така че съответните вътрешни и външни заинтересовани страни, включително външни доставчици на услуги, да бъдат информирани по своевременен и подходящ начин.

Насока 7: Тестване на мерките за сигурност

7.1 Доставчиците на платежни услуги следва да установят и въведат рамка за тестване, която да потвърждава изчерпателността и ефективността на мерките за сигурност и да гарантират, че рамката за тестване е адаптирана, така че да взема предвид новите заплахи и уязвимости, установени чрез дейностите за наблюдение на риска.

7.2 Доставчиците на платежни услуги следва да гарантират провеждането на тестовете в случай на промени на инфраструктурата, процесите или процедурите и ако са извършени промени като следствие от големи операционни инциденти или инциденти, свързани със сигурността.

7.3 Рамката за тестване следва също да обхваща мерките за сигурност, свързани с i) платежните терминали и устройства, които се използват за предоставянето на платежни услуги, ii) платежните терминали и устройства, които се използват за удостоверяване на ППУ и iii) устройствата и софтуера, предоставени от ДПУ на ППУ за генериране/получаване на код за удостоверяване на идентичността.

7.4 Рамката за тестване следва да гарантира, че тестовете:

а) се извършват като част от официалния процес за управление на промените на ДПУ, за да се гарантира тяхната изчерпателност и ефективност

б) се провеждат от независими проверяващи страни, които разполагат с достатъчни познания, умения и квалификация в областта на тестването на мерки за сигурност за платежни услуги и не са участвали в разработването на мерките за сигурност за съответните платежни услуги или системи, които ще бъдат тествани, най-малко за крайните тестове, преди въвеждането на мерките за сигурност; и

в) включват проверка на уязвимостите и тестове, свързани с проникване в системите, които да съответстват на нивото на установения риск за платежните услуги.

7.5 Доставчиците на платежни услуги следва да извършват редовни и повтарящи се тестове на мерките за сигурност за своите платежни услуги. За системите, които са от критично значение за предоставянето на платежните услуги (както е определено съгласно насока 3.2), тези тестове следва да се провеждат поне веднъж годишно. Некритичните системи следва да бъдат тествани редовно съгласно подход, базиран на риска, но най-малко веднъж на три години.

7.6 Доставчиците на платежни услуги следва да следят и оценяват резултатите от извършените тестове и съответно да обновяват своите мерки за сигурност без излишно забавяне по отношение на критичните системи.

Насока 8: Ситуационна осведоменост и непрекъснато обучение

Контекст на заплахите и ситуационна осведоменост

8.1 Доставчиците на платежни услуги следва да установят и въведат процеси и организационни структури за установяване и непрестанно наблюдение на заплахите за сигурността и операционните заплахи, които биха могли да окажат значително въздействие върху способността им да предоставят платежни услуги.

8.2 Доставчиците на платежни услуги следва да анализират операционните инциденти и инцидентите, свързани със сигурността, които са били установени или са възникнали в рамките на и/или извън организацията. Доставчиците на платежни услуги следва да вземат предвид натрупания от тези анализи опит и съответно да обновят мерките за сигурност.

8.3 Доставчиците на платежни услуги следва активно да следят технологичното развитие, за да гарантират, че са осведомени относно рисковете за сигурността.

Програми за обучение и осведоменост относно сигурността

8.4 Доставчиците на платежни услуги следва да въведат програма за обучение на целия персонал, за да гарантират, че е обучен да извършва задълженията и отговорностите си в съответствие с приложимите политики и процедури за сигурност, за да се намали риска от човешка грешка, кражба, измама, злоупотреба и загуба. Доставчиците на платежни услуги следва да гарантират, че програмата за обучение предоставя обучение на членовете на персонала най-малко веднъж годишно или по-често, ако е необходимо.

8.5 Доставчиците на платежни услуги следва да гарантират, че членовете на персонала, заемащи ключови длъжности съгласно насока 3.1 получават целево обучение относно сигурността на информацията веднъж годишно или по-често, ако е необходимо.

8.6 Доставчиците на платежни услуги следва да установят и провеждат периодични програми за осведоменост относно сигурността, за да обучават своя персонал и да обърнат внимание на рисковете, свързани с информационната сигурност. Тези програми следва да изискват от персонала на ДПУ да докладва за всички необичайни дейности и инциденти.

Насока 9: Управление на връзките с потребителите на платежни услуги

Осведоменост на потребителите на платежни услуги относно рисковете, свързани със сигурността, и действията за смекчаване на риска

9.1 Доставчиците на платежни услуги следва да установят и изпълняват процеси за повишаване на осведомеността на ППУ относно рисковете, свързани със сигурността при платежните услуги, като предоставят на ППУ помощ и насоки.

9.2 Помощта и насоките, които се предлагат на ППУ следва да бъдат обновявани в контекста на новите заплахи уязвимости и ППУ следва да бъдат уведомявани относно промените.

9.3 Когато функционалността на продукта позволява това, ДПУ следва да осигурят на ППУ възможност да деактивират определени функционалности за плащане, свързани с платежните услуги, предоставяни от ДПУ.

9.4 Когато в съответствие с член 68, параграф 1 от Директива (ЕС) 2015/2366 ДПУ са уговорили с платеца лимити за плащане за платежни операции, осъществявани чрез конкретни платежни инструменти, ДПУ следва да предоставят на платеца възможност да регулира тези ограничения до максималния договорен лимит.

9.5 Доставчикът на платежни услуги следва да предостави на ППУ възможност да получава известия за извършените и/или неуспешни опити за извършване на платежни операции, което да позволи на ППУ да установят измамна или злонамерена употреба на тяхната сметка.

9.6 Доставчикът на платежни услуги следва да информира ППУ относно обновяванията на процедурите по сигурността, които засягат ППУ по отношение на предоставянето на платежните услуги.

9.7 Доставчикът на платежни услуги следва да предостави на ППУ помощ за всички въпроси, искания за помощ и известия за нередности или проблеми, засягащи сигурността на платежните услуги. Потребителите на платежни услуги следва да бъдат достатъчно информирани относно това как могат да получат такава помощ.