EIOPA-BoS-20/600

Насоки за сигурността и управлението на информационно-комуникационните технологии

EIOPA – Westhafen Tower, Westhafenplatz 1 – 60327 Frankfurt – Германия – тел. + 49 69-951119-20;
факс + 49 69-951119-19; имейл: info@eiopa.europa.eu уеб сайт: www.eiopa.europa.eu

Съдържание

Предистория

1. Съгласно член 16 Регламент (ЕС) № 1094/2010 EIOPA може да издава насоки и препоръки до компетентните органи и финансови институции с оглед на това да се установят последователни, ефикасни и ефективни надзорни практики и да се гарантира общо, единно и последователно прилагане на законодателството на Съюза.

2. Съгласно член 16, параграф 3 от този регламент компетентните органи и финансовите институции трябва да полагат всички усилия за спазване на тези насоки и препоръки.

3. EIOPA идентифицира необходимостта от развитие на конкретни насоки за сигурността и управлението на информационно-комуникационните технологии (ИКТ) във връзка с членове 41 и 44 от Директива 2009/138/ЕО в контекста на анализа, извършен в отговор на План за действие в областта на финансовите технологии на Европейската комисия (оконч. COM(2018)0109), План за сближаване в областта на надзора 2018—2019 на EIOPA[1] и следните взаимодействия с няколко други заинтересовани страни[2].

4. Както се съобщава в Общите съвети на Европейските надзорни органи до Европейската комисия, Насоките на EIOPA относно системата на управление *„не отразяват подходящо важността от грижа за управление на риска в областта на ИКТ (вкл. кибернетичните рискове)*. Няма насоки по отношение на ключови елементи, които са общопризнати като част от подходящата сигурност и управление на ИКТ".

5. Анализът на текущата (законодателна) ситуация в ЕС за горепосочените Общи съвети показа, че по-голямата част от държавите — членки на ЕС, са определили национални правила за сигурността и управлението на ИКТ. Въпреки че изискванията са подобни, регулаторната рамка все още е фрагментирана. Освен това проучване върху текущите надзорни практики разкри голямо разнообразие от практики — от „няма конкретен надзор" до „строг надзор" (вкл. „дистанционни проверки" и „проверки на място").

6. Освен това сложността на ИКТ се увеличава и честотата на инцидентите, свързани с ИКТ (вкл. киберинцидентите), също се повишава, както и неблагоприятното въздействие на такива инциденти върху оперативното функциониране на предприятията. Поради тази причина управлението на риска в областта на ИКТ и сигурността е основополагащо, за да може едно предприятие да достигне своите стратегически, оперативни и свързани с репутацията цели.

7. Освен това в целия застрахователен сектор, включително в традиционните и в иновативните бизнес модели, все повече се разчита на ИКТ при предоставянето на застрахователни услуги и при нормалното оперативно функциониране на предприятията, напр. цифровата трансформация на застрахователния сектор (InsurTech, IoT и др.) и взаимосвързаността чрез телекомуникационни канали (интернет, мобилни и безжични връзки и широкообхватни мрежи). Това прави дейността на предприятията уязвима към инциденти, свързани със сигурността, включително на кибератаки. Затова е

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Докладът, публикуван от EIOPA в отговор на Плана за действие в областта на финансовите технологии на Европейската комисия, може да бъде намерен тук.

важно да се гарантира, че предприятията са адекватно подготвени за управление на рисковете в областта на ИКТ и сигурността.

8. Освен това, като признават необходимостта от подготвеност за кибернетичните рискове[3] и от стабилна рамка за киберсигурност от страна на предприятията, настоящите насоки обхващат също киберсигурността като част от мерките за информационна сигурност на предприятията. Докато настоящите насоки допускат, че киберсигурността следва да се разглежда като част от цялостното управление на риска в областта на ИКТ и сигурността, важно е да се отбележи, че кибератаките имат някои специфични характеристики, които трябва да се вземат предвид, за да се гарантира, че мерките за информационна сигурност намаляват адекватно киберриска:

   а) кибератаките често са по-трудни за управление (т.е. идентифициране, защита, откриване, реакция и пълно възстановяване) от повечето други източници на рискове в областта на ИКТ и сигурността и е трудно също така да се определи размерът на щетите;

   б) някои кибератаки могат да направят неефективни общото управление на риска и мерките за непрекъснатост на дейността, както и процедурите за възстановяване при бедствия, тъй като може да разпространят зловреден софтуер в системите за архивиране, за да ги направят недостъпни или да увредят архивираните данни;

   в) доставчици на услуги, брокери, (управляващи) агенти и посредници могат да станат канали за разпространение на кибератаки. Заразни тихи заплахи може да използват взаимосвързаност чрез телекомуникационни връзки на трета страна, за да стигнат до системата за ИКТ на предприятието. Затова взаимосвързано предприятие, което има индивидуална ниска значимост, може да стане уязвимо и източник на разпространение на риск и може да доведе до системно въздействие. При спазване на принципа за най-слабата връзка, киберсигурността не трябва да е грижа само на основните участници на пазара или на доставчиците на критични услуги.

9. Целта на настоящите насоки е да:

   а) предостави яснота и прозрачност на участниците на пазара за очаквания минимум информация и възможностите за киберсигурност, т.е. основните параметри за сигурността;

   б) избегне потенциален регулаторен арбитраж;

   в) насърчи сближаването в областта на надзора по отношение на очакванията и процесите, приложими във връзка със сигурността и управлението на ИКТ като начин за правилно управление на риска в областта на ИКТ и сигурността.

[3] За определение за кибернетичен риск вж. Киберлексикона на FSB, 12 ноември 2018 г. https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Насоки за сигурността и управлението на информационно-комуникационните технологии

Въведение

1. В съответствие с член 16 от Регламент (ЕС) № 1094/2010[4] EIOPA издава настоящите насоки до надзорните органи с цел предоставяне на напътствия относно начина, по който застрахователните и презастрахователните предприятия (събирателно „предприятия“) следва да прилагат изискванията към управлението, определени в Директива 2009/138/ЕО[5] (директива „Платежоспособност II“) и в Делегиран регламент (ЕС) № 2015/35 на Комисията[6] („Делегираният регламент“) в контекста на сигурността и управлението на информационно-комуникационните технологии (ИКТ). За тази цел настоящите насоки се основават на разпоредбите относно управлението, предвидени в членове 41, 44, 46, 47, 132 и 246 от Директива „Платежоспособност II“ и членове 258 до 260, 266, 268 до 271 и 274 на Делегирания регламент. Освен това настоящите насоки се основават също на напътствията в Насоки на EIOPA относно системата на управление (EIOPA-BoS-14/253)[7] и Насоки на EIOPA за възлагане на дейности на доставчици на услуги в облак (EIOPA-BoS-19/270)[8].

2. Насоките се прилагат за отделни предприятия и за *mutatis mutandis* на нивото на групата[9].

3. При спазването и наблюдаване на спазването на настоящите насоки компетентните органи следва да вземат предвид принципа на пропорционалност[10], който следва да гарантира, че мерките за управление, включително и тези, свързани със сигурността и управлението на ИКТ, са пропорционални на естеството, мащаба и сложността на съответните рискове, на които предприятията са изложени или могат да бъдат изложени.

4. Настоящите насоки следва да бъдат разглеждани във връзка със и без да се засяга Директива „Платежоспособност II“, Делегирания регламент, Насоките на EIOPA относно системата на управление и Насоките на EIOPA за възлагане на дейности на доставчици на услуги в облак Настоящите насоки имат за цел да са неутрални по отношение на технология и методология.

Определения

5. В случай че в настоящите насоки не е указано друго, термините имат значението, дефинирано в Директива „Платежоспособност II”.

6. За целите на настоящите насоки се прилагат следните определения:

---

[4] Регламент (ЕС) № 1094/2010 Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за застраховане и професионално пенсионно осигуряване), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/79/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 48).

[5] Директива 2009/138/ЕО Директива 2009/138/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. относно започването и упражняването на застрахователна и презастрахователна дейност (Платежоспособност II), (ОВ L 335, 17.12.2019 г., стр. 1).

[6] Делегиран регламент (ЕС) № 2015/35 на Комисията от 10 октомври 2014 г. за допълнение на Директива 2009/138/ЕО на Европейския парламент и на Съвета относно започването и упражняването на застрахователна и презастрахователна дейност (Платежоспособност II) (ОВ L 12, 17.1.2015 г., стр. 1).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] Член 212, параграф 1 от Директива 2009/138/ЕО

[10] Член 29, параграф 3 от Директива 2009/138/ЕО

Собственик на активи	Физическо или юридическо лице с отговорност и пълномощие за информационен актив и актив в областта на ИКТ.
Достъпност	Характеристика за достъпност и използваемост при поискване (своевременност) от упълномощен субект.
Поверителност	Характеристика за това, че информацията не е достъпна или разкрита на неупълномощени физически лица, субекти, процеси или системи.
Кибератака	Всеки вид хакерство, водещо до нападателен/злонамерен опит за унищожаване, излагане, промяна, дезактивиране, кражба или получаване на неоторизиран достъп или възползване от непозволена употреба на информационен актив, който е насочен към системи за ИКТ.
Киберсигурност	Запазване на поверителността, целостта и достъпността на информацията и/или на информационните системи чрез киберсреда.
Актив в областта на ИКТ	Актив на софтуер или хардуер, който се намира в бизнес средата.
Проекти в областта на ИКТ	Всеки проект или част от него, в който системите и услугите в областта на ИКТ се променят, заменят или прилагат.
Риск в областта на ИКТ и сигурността	Като подкомпонент на оперативния риск, рискът от загуба поради нарушаване на поверителността, нарушение на целостта на системи и данни, неприложимост или недостъпност до системи и данни, или невъзможност за промяна на ИКТ в разумен срок и с разумни разходи, когато изискванията на средата или дейността се променят (т.е. бързина на извършване на промяна). Това включва кибернетични рискове, както и рискове за информационната сигурност, произтичащи от неподходящи или неуспешни вътрешни процеси или външни събития, включително кибератаки или недостатъчна физическа сигурност.

Информационна сигурност	Запазване на поверителността, целостта и достъпността на информацията и/или на информационните системи. Освен това може да бъдат включени други характеристики като автентичност, подотчетност, невъзможност за непризнаване и надеждност.
Услуги в областта на ИКТ	Услуги, предоставяни от системи за ИКТ и доставчици на услуги за един или повече вътрешни или външни потребители.
ИКТ системи	Набор от приложения, услуги, активи в областта на информационните технологии, активи в областта на ИКТ или други обработващи информация компоненти, които включва оперативната среда.
Информационен актив	Съвкупност от информация, материална или нематериална, която е важно да бъде защитена.
Цялост	Характеристика за точност и пълнота.
Оперативни инциденти или инциденти, свързани със сигурността	Единично събитие или поредица от свързани непланирани събития, които оказват или вероятно ще окажат неблагоприятно въздействие върху целостта, достъпността и поверителността на системите и услугите в областта на ИКТ.
Доставчик на услуга	Означава субект трета страна, който извършва процес, услуга или дейност или части от тях по силата на споразумение за възлагане на дейности на външни изпълнители.
Тестване за проникване на заплаха	Контролиран опит за компрометиране на киберустойчивостта на субект чрез симулиране на тактики, техники и процедури на реални източници на заплахи. Базира се на разузнаването за целенасочена заплаха и се фокусира върху служителите, процесите и технологията на субекта, с минимално предварително познание и въздействие върху дейността.
Уязвимост	Слаба страна, податливост или дефект на актив или контрол, който може да се експлоатира от една или повече заплахи.

7. Настоящите насоки влизат в сила от 1 юли 2021 г.

Насока 1 — Пропорционалност

8. Предприятията следва да прилагат настоящите насоки по начин, който е пропорционален на естеството, мащаба и сложността на рисковете, свързани с тяхната дейност.

Насока 2 — ИКТ в рамките на системата на управление

9. Административният, управителният или надзорният орган (АУНО) следва да гарантира, че системата на управление на предприятията, по-специално управлението на риска и системата за вътрешен контрол, управляват адекватно рисковете в областта на ИКТ и сигурността.

10. АУНО следва да гарантира, че количеството и уменията на персонала на предприятията са адекватни за поддържане на техните оперативни нужди, процеси на управление на риска в областта на ИКТ и сигурността постоянно и да гарантира изпълнението на тяхната стратегия в областта на ИКТ. Освен това персоналът следва да получава адекватно обучение за рисковете в областта на ИКТ и сигурността, включително и за информационната сигурност, редовно, както е определено в Насока 13.

11. АУНО следва да гарантира, че разпределените ресурси са подходящи за изпълнение на горепосочените изисквания.

Насока 3 — Стратегия за ИКТ

12. АУНО носи цялостна отговорност за определяне и одобряване на писмената стратегия на предприятията в областта на ИКТ като част от цялостната им бизнес стратегия и приведени в съответствие с нея, както и за надзор над комуникацията и изпълнението.

13. Стратегията в областта на ИКТ следва да определя най-малкото:

    а) по какъв начин трябва да се развиват ИКТ на предприятията, за да подпомагат и изпълняват ефективно своята бизнес стратегия, включително развитието на организационната структура, бизнес модели, системата за ИКТ и ключови зависимости от доставчици на услуги;

    б) еволюцията на архитектурата на ИКТ, включително зависимости от доставчици на услуги; и

    в) ясни цели, свързани с информационната сигурност, с акцент върху системите и услугите за ИКТ, персонала и процесите.

14. Предприятията следва да гарантират, че стратегията в областта на ИКТ е приложена, приета и съобщена на целия съответен персонал и доставчици на услуги, както е приложимо и релевантно, своевременно.

15. Предприятията трябва да установят процес за наблюдение и измерване на ефективността на изпълнението на стратегията в областта на ИКТ. Този процес трябва да бъде преразглеждан и актуализиран редовно.

Насока 4 — Рискове в областта на ИКТ и сигурността в рамките на системата за управление на риска

16. АУНО носи цялостна отговорност за установяване на ефективна система за управление на рисковете в областта на ИКТ и сигурността като част от цялостната система за управление на риска на предприятието. Това включва определянето на допустим риск за тези рискове, съгласно стратегията за риска

на предприятието, и регулярен писмен доклад до АУНО относно резултата от процеса на управление на риска.

17. Като част от цялостната им система за управление на риска, предприятията следва, във връзка с рисковете в областта на ИКТ и сигурността (докато дефинират изискванията за защита на ИКТ, така както е описано по-долу), да вземат предвид най-малко следното:

    а) предприятията следва да установят и редовно да актуализират съпоставянето на своите стопански процеси и дейности, стопански функции, роли и активи (напр. информационните активи и активите в областта на ИКТ), за да установят тяхната важност и взаимозависимости от рискове в областта на ИКТ и сигурността.

    б) предприятията следва да установяват и измерват всички съответни рискове в областта на ИКТ и сигурността, на които са изложени, и да класифицират идентифицираните стопански процеси и дейности, стопански функции, роли и активи (напр. информационните активи и активите в областта на ИКТ) по отношение на критичността. Предприятията следва също да оценяват изискванията за защита най-малкото на поверителността, целостта и достъпността на тези стопански процеси и дейности, стопански функции, роли и активи (напр. информационните активи и активите в областта на ИКТ). Собствениците на активи, които са отговорни за класификацията на активите, следва да бъдат установени;

    в) методите, използвани за определяне на критичността, както и необходимото ниво на защита, по-специално във връзка с целите за защитата на целостта, наличността и поверителността, следва да гарантират, че произтичащите изисквания за защита са последователни и изчерпателни;

    г) измерването на рискове в областта на ИКТ и сигурността следва да се извършва на базата на определените критерии за рискове в областта на ИКТ и сигурността, като се вземе предвид критичността на техните стопански процеси и дейности, стопански функции, роли и активи (напр. информационните активи и активите в областта на ИКТ), степента на известните към момента уязвимости и предходни инциденти, които са оказали въздействие върху предприятието;

    д) оценката на риска в областта на ИКТ и сигурността следва да се извършва и документира редовно. Тази оценка трябва също да се извършва преди всяка основна промяна в инфраструктурата, процесите или процедурите, влияещи върху стопанските процеси и дейности, стопанските функции, ролите и активите (напр. информационните активи и активите в областта на ИКТ);

    е) въз основа на оценката на риска предприятията следва най-малкото да определят и приложат мерки за управление на идентифицираните рискове в областта на ИКТ и сигурността и да защитят информационните активи съгласно класификацията им. Това трябва да включва определението на мерките на оставащите остатъчни рискове.

18. Резултатите от процеса на управление на риска в областта на ИКТ и сигурността следва да бъдат одобрени от АУНО и да бъдат включени в процеса на оперативното управление на риска като част от цялостното управление на риска на предприятието.

Насока 5 — Одит

19. Управлението, системите и процесите, възприети от предприятията по отношение на рисковете в областта на ИКТ и сигурността, следва да бъдат одитирани периодично в съответствие с плана за одит на предприятията[11] от одитори с достатъчно знания, умения и експертен опит от рискове в областта на ИКТ и сигурността, за да се предостави независима гаранция за тяхната ефективност пред АУНО. Честотата и фокусът на такива одити трябва да бъдат съизмерими със съответните рискове в областта на ИКТ и сигурността.

Насока 6 — Политика и мерки за информационна сигурност

20. Предприятията следва да установят писмена политика за информационна сигурност, одобрена от АУНО, която следва да определи основни принципи и правила за защита на поверителността, целостта и достъпността на информацията за предприятията, за да се поддържа прилагането на стратегията в областта на ИКТ.

21. Политиката следва да включва описание на основните роли и отговорности за управлението на информационната сигурност и да определя изискванията към персонала, процесите и технологиите във връзка с информационната сигурност, като се признава, че персоналът на всички равнища има отговорности за гарантиране на информационната сигурност на предприятията.

22. Политиката следва да бъде съобщена в предприятието и да се прилага за целия персонал. Когато е приложимо и подходящо, политиката за информационна сигурност или нейни части следва също да бъдат съобщени и приложени по отношение на доставчиците на услуги.

23. На базата на политиката предприятията следва да установят и приложат по-специфични процедури за информационна сигурност и мерки за информационна сигурност, *inter alia*, да ограничат рисковете в областта на ИКТ и сигурността, на които са изложени. Тези процедури и мерки за информационна сигурност следва да включват всеки един процес, описан в настоящите насоки, както е приложимо.

Насока 7 — Функция за информационна сигурност

24. Предприятията следва да установят в рамките на своята системата на управление и в съответствие с принципа на пропорционалността, функция за информационна сигурност, като отговорностите са възложени на определено лице. Предприятието следва да гарантира независимостта и обективността на функцията за информационна сигурност, като я отдели по подходящ начин от процесите, свързани с дейността и развитието в областта на ИКТ. Функцията следва да докладва на АУНО.

25. Задачите на функцията за информационна сигурност обикновено са:

    а) да подпомага АУНО при определянето и поддръжката на политиката за информационна сигурност за предприятията и да контролира прилагането ѝ;

    б) да докладва на АУНО и да иска съвети от него редовно, на *ad hoc* основа, за състоянието на информационната сигурност и нейното развитие;

[11] Член 271 от Делегирания регламент.

в) да наблюдава и да прави преглед на изпълнението на мерките за информационна сигурност;

г) да гарантира, че изискванията за информационна сигурност се спазват при използване на доставчици на услуги;

д) да гарантира, че всички служители и доставчици на услуги, които имат достъп до информация и системи са адекватно информирани относно политиката за информационна сигурност, например чрез обучение за информационна сигурност и сесии за повишаване на осведомеността;

е) да координира проверката на оперативни инциденти или инциденти, свързани със сигурността и да докладва за съответните инциденти на АУНО.

Насока 8 — Логическа сигурност

26. Предприятията следва да определят, документират и прилагат процедури за логически контрол на достъпа или логическа сигурност (идентичност и управление на достъпа) в съответствие с изискванията за защита, както е определено в Насока 4. Тези процедури следва да бъдат въвеждани, прилагани, наблюдавани и периодично оценявани и следва също да включват контрол за мониторинг на аномалии. Тези процедури следва да прилагат най-малко следните елементи, като терминът „потребител" включва и техническите потребители:

а) необходимост да се знае, най-малка привилегия и разделяне на задълженията: предприятията следва да управляват правата за достъп, включително отдалечения достъп до информационни активи и техните поддържащи системи въз основа на принципа „необходимост да се знае". На потребителите следва да се предоставят права за минимален достъп, които са строго необходими за изпълнение на техните задължения (принцип на „най-малка привилегия"), т.е. да се предотврати неправомерен достъп до данни или да се предотврати разпределянето на комбинации от права на достъп, които могат да се използват за заобикаляне на мерките за контрол (принцип на „разделяне на функциите");

б) отчетност на потребителите: предприятията следва да ограничат, доколкото е възможно, използването на общи и споделени потребителски акаунти и да гарантират, че потребителите могат да бъдат идентифицирани и проследявани до отговорно физическо лице или разрешена задача за осъществените действия в системите за ИКТ по всяко време;

в) права за привилегирован достъп: предприятията следва да осъществяват строг контрол върху привилегирования достъп до системата чрез строго ограничаване и строго наблюдение на акаунтите с повишени права на достъп до дадена система (напр. акаунти на администратори);

г) отдалечен достъп: за да се гарантира сигурността на комуникациите и да се намали рискът, отдалеченият административен достъп до критични системи за ИКТ следва да се предоставя само на принципа „необходимост да се знае" и когато се използват сигурни решения за удостоверяване на самоличността;

д) регистриране на потребителски дейности: потребителските дейности следва да бъдат входирани и наблюдавани по начин, който е

пропорционален на риска, като включват най-малко дейности на привилегировани потребители. Регистрите на достъпа следва да бъдат предпазвани с цел предотвратяване на неразрешено изменение или заличаване и съхранявани за период, който е съизмерим с критичността на определените стопански функции, помощни процеси и информационни активи, без да се засягат изискванията за запазване, определени в законодателството на ЕС и националното законодателство. Предприятията следва да използват тази информация за улесняване на установяването и разследването на неправомерни действия, които са били открити при предоставянето на услуги;

е) управление на достъпа: права за достъп трябва да се дават, премахват и променят своевременно съгласно предварително определени практики за одобрение, когато е включен собственикът на приложимите информационни активи. В случай, че повече не се изисква достъп, правата за достъп следва да бъдат отменени незабавно;

ж) оценка на достъпа: правата за достъп следва да се преразглеждат периодично, за да се гарантира, че потребителите не притежават прекомерни привилегии и правата за достъп са оттеглени/премахнати, когато вече не са необходими;

з) даването, промяната, анулирането на права за достъп следва да се документира по начин, който улеснява разбирането и анализа; и

и) методи за удостоверяване на автентичността: предприятията следва да прилагат методи за удостоверяване на автентичността, които са достатъчно надеждни, за да гарантират адекватно и ефективно спазване на политиките и процедурите за контрол на достъпа. Методите за удостоверяване на автентичността следва да бъдат съизмерими с критичността на системите за ИКТ, информацията или процеса, до който се осъществява достъп. Това следва да включва като минимум силни пароли или по-строги методи за удостоверяване на автентичността (напр. двуфакторно удостоверяване), основани на съответния риск.

27. Електронният достъп чрез приложения до системите за данни и ИКТ следва да бъде ограничен до минимално необходимото за предоставяне на съответната услуга.

Насока 9 — Физическа сигурност

28. Мерки за физическа сигурност на предприятията (напр. защита срещу прекъсване на електрозахранването, пожар, вода и неоторизиран физически достъп) следва да се определят, документират и прилагат за защита на техните помещения, центрове за данни и чувствителни зони от неразрешен достъп и от опасностите за околната среда.

29. Физическият достъп до системи за ИКТ следва да бъде предоставян само на упълномощени лица. Упълномощаването следва да се предоставя в съответствие със задачите и отговорностите на физическите лица и да се ограничава до физическите лица, които са подходящо обучени и наблюдавани. Физическият достъп следва редовно да се преразглежда, за да се гарантира, че ненужните права за достъп се оттеглят/премахват незабавно.

30. Подходящите мерки за защита от опасности, свързани с околната среда, следва да бъдат съизмерими със значението на сградите и критичността на дейността или на системите за ИКТ, намиращи се в тези сгради.

Насока 10 — Сигурност на дейността в областта на ИКТ

31. Предприятията следва да прилагат процедури, за да се гарантира поверителността, целостта и достъпността на системите за ИКТ и услугите за ИКТ, за да се сведе съответно до минимум въздействието на проблеми със сигурността при доставката на услуги за ИКТ. Тези процедури следва да включват по подходящ начин следните мерки:

    а) установяване на потенциални уязвимости, които следва да се оценяват и коригират, като се гарантира актуалността на системите за ИКТ, включително софтуера, предоставен от предприятията на техните вътрешни и външни потребители, чрез разполагане на критични защитни елементи, включително актуализации на антивирусни дефиниции или чрез прилагане на компенсаторни мерки за контрол;

    б) прилагане на базова линия за защитено конфигуриране за всички критични компоненти като операционни системи, бази данни, рутери или комутатори;

    в) осъществяване на сегментиране на мрежата, системите за предотвратяване на изтичане на данни и шифроване на мрежовия трафик (в съответствие с класификацията на информационните активи);

    г) прилагане на защита на крайни точки, включително сървъри, работни станции и мобилни устройства. Предприятията следва да оценяват дали една крайна точка отговаря на стандартите за сигурност, определени от тях, преди да ѝ се даде достъп до корпоративната мрежа;

    д) гарантиране наличието на механизми за проверка на целостта, за да се провери целостта на системите за ИКТ;

    е) шифроване на данните в режим на покой и в режим на движение (в съответствие с класификацията на информационните активи).

Насока 11 — Мониторинг на сигурността

32. Предприятията следва да установят и прилагат процедури и процеси за продължителен мониторинг на дейностите, които оказват въздействие върху информационната сигурност на предприятията. Мониторингът следва да обхваща най-малко:

    а) вътрешни и външни фактори, включително стопански функции и административни функции, свързани с ИКТ;

    б) трансакции от доставчици на услуги, други субекти и вътрешни потребители; и

    в) потенциални вътрешни и външни заплахи.

33. Въз основа на мониторинга предприятията следва да приложат подходящи и ефективни възможности за откриване, докладване и отговор на неправомерни действия и заплахи, например физическо или логическо проникване, нарушаване на поверителността, целостта и достъпността на информационни активи, злонамерен код и публично известни уязвимости за софтуера и хардуера.

34. Докладването във връзка с мониторинга на сигурността следва да помогне на предприятията да разберат естеството на оперативните инциденти и на инцидентите, свързани със сигурността, да идентифицират тенденции и да

подпомогне вътрешните разследвания на предприятията, както и да им даде възможност да вземат подходящи решения.

Насока 12 — Прегледи, оценка и проверка на информационната сигурност

35. Предприятията следва да извършват различни прегледи, оценки и проверки на информационната сигурност, за да се гарантира ефективното идентифициране на уязвимостите в техните системи и услуги за ИКТ. Например, предприятията могат да извършват анализ на пропуските въз основа на стандартите за информационна сигурност, прегледи за съответствие, вътрешни и външни одити на информационните системи или прегледи на физическата сигурност.

36. Предприятията следва да установят и прилагат рамка за проверка на информационната сигурност, която да утвърждава надеждността и ефективността на мерките за информационна сигурност, и да гарантират, че в тази рамка са взети под внимание заплахите и уязвимостите, установени чрез наблюдение на заплахите и процеса на оценка на риска в областта на ИКТ и сигурността.

37. Проверката следва да се осъществява по безопасен и сигурен начин и чрез независими тестващи потребители с достатъчно знания, умения и експертен опит при проверката на мерки за информационна сигурност.

38. Предприятията следва да извършват проверки редовно. Обхватът, честотата и методът на проверката (напр. проверка за проникване, включително проверка за проникване на заплаха) следва да са съизмерими с нивото на установения риск. Проверката на критичните системи за ИКТ и сканирането за уязвимости следва да се извършват ежегодно.

39. Предприятията следва да гарантират, че се извършват проверки на мерките за сигурност в случай на промени в инфраструктурата, процесите или процедурите и ако са направени промени поради големи оперативни инциденти или инциденти, свързани със сигурността, или поради пускането на нови или значително променени критични приложения. Предприятията следва да наблюдават и оценяват резултатите от проверките на сигурността и съответно да актуализират своите мерки за сигурност без необосновано забавяне, в случай на критични системи за ИКТ.

Насока 13 — Обучение за информационна сигурност и повишаване на осведомеността

40. Предприятията следва да изготвят програми за обучение за информационна сигурност за целия персонал, включително АУНО, за да се гарантира, че персоналът е обучен да изпълнява задълженията и отговорностите си, за да се намалят случаите на човешка грешка, кражба, измама, злоупотреба или загуба. Предприятията следва да гарантират, че програмата за обучение предоставя обучение за целия персонал редовно.

41. Предприятията следва да изготвят и прилагат периодични програми за повишаване на осведомеността относно сигурността, за да обучат персонала си, включително АУНО, за това как да се справя с рисковете, свързани с информационната сигурност.

Насока 14 — Управление на дейността в областта на ИКТ

42. Предприятията следва да управляват дейността си в областта на ИКТ на базата на стратегия в областта на ИКТ. Документите следва да определят как предприятията експлоатират, наблюдават и контролират системите и услугите за ИКТ, включително документирането на критични процеси, процедури и дейност в областта на ИКТ.

43. Предприятията следва да прилагат процедури за регистриране и наблюдение за критична дейност в областта на ИКТ, за да се даде възможност за откриване, анализ и коригиране на грешки.

44. Предприятията следва да поддържат актуализирана инвентаризация на активите си в областта на ИКТ. Инвентаризацията на активите в областта на ИКТ следва да бъде достатъчно подробна, за да позволи бързото идентифициране на актив в областта на ИКТ, неговото местоположение, класификацията за сигурност и собственост.

45. Предприятията следва да наблюдават и управляват жизнения цикъл на активите в областта на ИКТ, за да се гарантира, че продължават да отговарят на изискванията за дейността и за управлението на риска и да ги подпомагат. Предприятията следва да наблюдават дали активите им в областта на ИКТ се подпомагат от търговците или вътрешните разработчици, както и дали всички съответни корекции и актуализации се прилагат въз основа на документирани процеси. Рисковете, произтичащи от остарели или неподдържани активи в областта на ИКТ, следва да се оценяват и ограничават. Изведените от експлоатация активи в областта на ИКТ следва да бъдат безопасно обработени и освободени.

46. Предприятията следва своевременно да прилагат процеси за планиране на изпълнението и капацитета и наблюдение с цел предотвратяване, откриване и реагиране на важни проблеми във връзка с ефективността на системите за ИКТ и недостига на капацитет в областта на ИКТ.

47. Предприятията следва да определят и прилагат процедури за възстановяване и архивиране на данни и системи за ИКТ, за да се гарантира, че те могат да бъдат възстановени съгласно изискванията. Обхватът и честотата на архивните копия следва да бъдат определени в съответствие с изискванията за възстановяване на дейността и критичността на данните и системите за ИКТ, както и да бъдат оценявани в съответствие с извършената оценка на риска. Редовно следва да се извършва проверка на процедурите за създаване на архивни копия и възстановяване.

48. Предприятията следва да гарантират, че архивните копия на данните и системите за ИКТ се съхраняват на едно или повече местоположения, които са извън основното място и са надеждни и достатъчно отдалечени от основното място, за да се избегне излагането им на едни и същи рискове.

Насока 15 — Управление на инциденти и проблеми в областта на ИКТ

49. Предприятията следва да установят и прилагат процес на управление на инциденти и проблеми, за да наблюдават и регистрират оперативните или свързаните със сигурността инциденти, което да позволи на предприятията да продължат или да възобновят критични стопански функции и процеси при възникване на смущения.

50. Предприятията следва да определят подходящи критерии и прагове за класифициране на дадено събитие като оперативен инцидент или инцидент,

свързан със сигурността, както и индикатори за ранно предупреждение, които следва да служат за известяване, което да позволи ранно откриване на тези инциденти.

51. За да се сведе до минимум въздействието на неблагоприятните събития и да се даде възможност за своевременно възстановяване, предприятията следва да установят подходящи процеси и организационни структури, за да се гарантира последователно и интегрирано наблюдение, обработка и последващи действия по отношение на оперативните инциденти и инцидентите, свързани със сигурността, както и да се гарантира, че основните причини са установени, отстранени и са предприети коригиращи действия/мерки за предотвратяване на повтарящи се инциденти. При процеса на управление на инциденти и проблеми следва да се осъществяват най-малкото:

    а) процедурите за идентифициране, проследяване, регистриране, категоризиране и класифициране на инциденти по даден приоритет, определен от предприятието и въз основа на критичността на дейността и споразуменията за услуги;

    б) ролите и отговорностите за различните сценарии на инциденти (напр. грешки, неизправности, кибератаки);

    в) процедура за управление на проблеми с цел установяване, анализиране и разрешаване на първопричините за един или повече инциденти; предприятията следва да анализират оперативни инциденти и инциденти, свързани със сигурността, които са били установени или са възникнали в организацията и/или извън нея, и да вземат предвид основните поуки, извлечени от тези анализи, и съответно да актуализират мерките за сигурност;

    г) ефективни планове за вътрешна комуникация, включително уведомяване за инциденти и процедури за ескалация, които обхващат също жалби на клиенти, свързани със сигурността, за да се гарантира, че:

        i. инциденти с потенциално силно неблагоприятно въздействие върху критични системи и услуги за ИКТ се докладват на съответното висше ръководство;

        ii. АУНО се информира на *ad hoc* основа в случай на значими инциденти и се информира най-малкото за въздействието, отговора и допълнителните проверки, които ще бъдат определени в резултат на инцидентите.

    д) процедури за реагиране при инциденти, за да се намали въздействието, свързано с инцидентите, и да се гарантира, че услугата своевременно започва да функционира и става сигурна;

    е) специфични планове за външна комуникация за критични стопански функции и процеси с цел:

        i. сътрудничество със съответните заинтересовани страни, за да могат ефективно да реагират на инцидента и да се възстановят от него;

        ii. своевременно предоставяне на информация, включително докладване за инциденти, на външни страни (напр. клиенти, други участници на пазара, съответните (надзорни) органи по целесъобразност и в съответствие с приложимата разпоредба).

Насока 16 — Управление на проекти в областта на ИКТ

52. Предприятията следва да прилагат методология за проекти в областта на ИКТ (вкл. независими съображения за изисквания за сигурност) с адекватен процес на управление и ръководство за изпълнение на проекти, за да се подпомага ефективно прилагането на стратегията в областта на ИКТ чрез проекти в областта на ИКТ.

53. Предприятията следва да наблюдават по подходящ начин и да ограничават рисковете, произтичащи от портфейла на проектите в областта на ИКТ, като вземат предвид и рисковете, които могат да възникнат от взаимозависимостите между различни проекти и от зависимостите от множество проекти върху същите ресурси и/или експертен опит.

Насока 17 — Придобиване и разработване на системи за ИКТ

54. Предприятията следва да развиват и прилагат процес за управление на придобиването, разработването и поддръжката на системи за ИКТ, за да гарантират, че поверителността, целостта, достъпността на данните за обработка са защитени напълно и са спазени определените изисквания за защита. Този процес следва да бъде разработен чрез използване на основан на риска подход.

55. Предприятията следва да гарантират, че преди да се осъществят дейности във връзка с придобиване и разработване на системи, функционалните и нефункционалните изисквания (вкл. изискванията за информационна сигурност) и техническите цели са ясно определени.

56. Предприятията следва да гарантират, че са налице мерки за предотвратяване на неумишлена промяна или умишлена манипулация на системите за ИКТ по време на разработването.

57. Предприятията следва да имат налична методология за тестване и одобрение на системи за ИКТ, услуги за ИКТ и мерки за информационна сигурност.

58. Предприятията следва по подходящ начин да тестват системите за ИКТ, услугите за ИКТ и мерките за информационна сигурност, за да откриват потенциални слабости в сигурността, нарушения и инциденти.

59. Предприятията следва да гарантират отделянето на производствената среда от развитието, тестването и други непроизводствени среди.

60. Предприятията следва да прилагат мерки за защита на изходния код (ако е наличен) за системите за ИКТ. Те следва също да документират разработването, прилагането, функционирането и/или конфигурацията на системите за ИКТ изчерпателно, за да се намали ненужната зависимост от експерти по темата.

61. Процесите на предприятията за придобиване и разработване на системи за ИКТ следва да се прилагат и за системи за ИКТ, разработени или управлявани от крайните потребители на стопанската функция извън организацията на ИКТ (напр. приложения, управлявани от стопанската единица или приложения за крайни потребители), като се използва основан на риска подход. Предприятията следва да поддържат регистър на тези приложения, които поддържат критични стопански функции или процеси.

Насока 18 — Управление на промени в областта на ИКТ

62. Предприятията следва да установят и прилагат процес на управление на промените в областта на ИКТ, за да гарантират, че всички промени в системите

за ИКТ се записват, оценяват, тестват, одобряват, разрешават и прилагат по контролиран начин. Промени по време на неотложни или извънредни промени в областта на ИКТ следва да са проследяеми и с последващо уведомяване на съответния собственик на активи за последващ анализ.

63. Предприятията следва да определят дали промените в съществуващата оперативна среда влияят на съществуващите мерки за сигурност или да изискват приемането на допълнителни мерки за намаляване на съответните рискове. Тези промени следва да бъдат в съответствие с официалния процес на управление на промените от страна на предприятията.

Насока 19 — Управление на непрекъснатостта на дейността

64. Като част от цялостната политика за непрекъснатост на дейността на предприятията, АУНО е отговорен за определяне и одобряване на политиката за непрекъснатост на ИКТ на предприятията. Политиката за непрекъснатост на ИКТ следва да бъде съобщена по подходящ начин в предприятията и да се прилага за целия съответен персонал и, ако е необходимо, на доставчици на услуги.

Насока 20 — Анализ на въздействието върху дейността

65. Като част от доброто управление на непрекъснатостта на дейността, предприятията следва да правят анализ на въздействието върху дейността, за да оценят излагането на сериозни смущения в дейността и потенциалното им въздействие, количествено и качествено, чрез използване на вътрешни и/или външни данни и анализ на сценарии. При анализа на въздействието върху дейността следва също да се вземе предвид критичността на идентифицираните и класифицираните стопански процеси и дейности, стопански функции, роли и активи (напр. информационните активи и активите в областта на ИКТ) и техните взаимозависимости съгласно Насока 4.

66. Предприятията следва да гарантират, че системите им за ИКТ и услуги за ИКТ са проектирани и приведени в съответствие с анализа на въздействието върху дейността, например с резерв от някои критични компоненти, за да се предотвратяват смущения, причинени от събития, които оказват въздействие върху тези компоненти.

Насока 21 — Планиране на непрекъснатостта на дейността

67. Цялостните планове за непрекъснатост на дейността (ПНД) на предприятията следва да вземат предвид материалните рискове, които могат да окажат неблагоприятно въздействие върху системите за ИКТ и услугите за ИКТ. Плановете следва да подпомагат целите за защита и, ако е необходимо, да възстановят поверителността, целостта и достъпността на стопанските процеси и дейности, стопанските функции, роли и активи (напр. информационните активи и активите в областта на ИКТ) на предприятията. При изготвянето на тези планове предприятията следва да се координират със съответните вътрешни и външни заинтересовани страни по целесъобразност.

68. Предприятията следва да въведат ПНД, за да гарантират, че могат да реагират по подходящ начин на потенциални неблагоприятни сценарии в целевия срок за възстановяване (максималното време, през което процес или система трябва да бъде възстановен(а) след инцидент) и целевата точка за възстановяване (максималният времеви период, през който може да се загубят данни в случай на инцидент на предварително определено ниво на услуги).

69. Предприятията следва да вземат предвид набор от различни сценарии в ПНД, включително крайни, но реалистични сценарии и сценарии за кибератаки и да оценяват потенциалното въздействие на такива сценарии. На базата на тези сценарии предприятията следва да опишат как се гарантира непрекъснатостта на системите и услугите за ИКТ, както и информационната сигурност на предприятията.

Насока 22 — Планове за ответна реакция и възстановяване

70. Въз основа на анализа на въздействието върху дейността и на реалистичните сценарии предприятията следва да разработят планове за ответна реакция и възстановяване. В тях трябва да бъдат посочени условията, които могат да доведат до задействане на плана, както и действията, които следва да се предприемат, за да се гарантират целостта, достъпността, непрекъснатостта и възстановяването най-малкото на критичните системи за ИКТ, услугите за ИКТ и данните на предприятията. Плановете за ответна реакция и възстановяване следва да са насочени към постигане на целите за възстановяване на дейността на предприятията.

71. В плановете за ответна реакция и възстановяване следва да се разглеждат краткосрочни и, ако е необходимо, дългосрочни варианти за възстановяване. Плановете следва най-малкото:

    а) да са фокусирани върху възстановяване на дейността на важни услуги за ИКТ, стопански функции, поддържащи процеси, информационни активи и техните взаимозависимости, за да се избегне неблагоприятното въздействие върху функционирането на предприятието;

    б) да бъдат документирани и достъпни за стопанските и поддържащите единици и леснодостъпни при спешни случаи, включително с ясно определяне на ролите и отговорностите; и

    в) да се актуализират непрекъснато в съответствие с поуките, извлечени от инциденти, проверки, нови установени рискове и заплахи, и променени цели и приоритети по отношение на възстановяването.

72. В плановете следва също да се разглеждат алтернативни варианти, при които възстановяването може да не е осъществимо в краткосрочен план поради разходи, рискове, логистични или непредвидени обстоятелства.

73. Като част от плановете за ответна реакция и възстановяване, предприятията трябва да обмислят и въведат мерки за непрекъснатост, за да ограничат неуспеха на доставчици на услуги, които са от ключово значение за непрекъснатостта на услугите за ИКТ на предприятията (в съответствие с разпоредбите на Насоките на EIOPA относно системата на управление и Насоките на EIOPA за възлагане на дейности на доставчици на услуги в облак).

Насока 23 — Тестване на плановете

74. Предприятията следва да тестват своите ПНД и да гарантират, че дейността на критичните стопански процеси и дейности, стопански функции, роли и активи (напр. информационни активи) и активите в областта на ИКТ и техните взаимозависимости (вкл. тези, които са предоставени от доставчици на услуги) се тестват редовно въз основа на рисковия профил на предприятията.

75. ПНД следва да се актуализират редовно, въз основа на резултатите от тестовете, настоящата информация относно заплахите и поуките, извлечени от предишни събития. Всички съответни промени на целите за възстановяване

(вкл. целевият срок за възстановяване и целевата точка за възстановяване) и/или промени на стопански процеси и дейности, стопански функции, роли и активи (напр. информационните активи и активите в областта на ИКТ), следва също да бъдат включени.

76. Тестването на ПНД следва да покаже, че те са способни да поддържат жизнеспособността на дейността до възстановяването на критичната дейност на предварително определено ниво на услуги или да въздействат на допустимото отклонение.

77. Резултатите от тестовете следва да бъдат документирани и всички установени недостатъци, произтичащи от тестовете, да бъдат анализирани, разгледани и докладвани на АУНО.

Насока 24 — Комуникация при кризисни ситуации

78. В случай на смущение или извънредна ситуация и при изпълнението на ПНД, предприятията следва да гарантират, че разполагат с въведени ефективни мерки за комуникация при кризисни ситуации, така че всички съответни вътрешни и външни заинтересовани страни, включително съответните надзорни органи, когато се изисква от национална разпоредба, както и съответните доставчици на услуги, са информирани по своевременен и подходящ начин.

Насока 25 — Възлагане на услуги за ИКТ и системи за ИКТ на външни изпълнители

79. Без да се засягат Насоките на EIOPA за възлагане на дейности на доставчици на услуги в облак, предприятията следва да гарантират, че при възлагането на услуги за ИКТ и системи за ИКТ на външни изпълнители са изпълнени съответните изисквания за услуга за ИКТ или система за ИКТ.

80. В случай на възлагане на критични или важни функции на външни изпълнители, предприятията следва да гарантират, че в договорните задължения на доставчика на услуги (напр. договор, споразумения за нива на услуги, разпоредби за прекратяване в съответните договори) е включено най-малко следното:

    а) подходящи и пропорционални цели и мерки за информационна сигурност, включително изисквания като минимални изисквания за информационна сигурност, спецификации на жизнения цикъл на данните на предприятията, права за одит и достъп и всякакви изисквания относно местоположението на центрове за данни и изисквания за шифроване на данни, защита на мрежата и процеси за мониторинга на сигурността;

    б) споразумения за нива на услуги, за да се гарантира непрекъснатостта на услугите и системите за ИКТ, както и очакваните резултати при нормални обстоятелства и тези, които се предоставят чрез планове за действие при извънредни ситуации, в случай на прекъсване на услуга; и

    в) оперативни процедури и процедури за справяне с инциденти, включително ескалация и докладване.

81. Предприятията следва да следят и да търсят потвърждение за нивото на съответствие на тези доставчици на услуги с техните цели, мерки и очаквани резултати по отношение на сигурността.

Правила за нормативно съответствие и за докладване

82. Този документ съдържа насоки, издадени съгласно член 16 от Регламент (ЕС) № 1094/2010. Съгласно член 16, параграф 3 от този регламент компетентните органи и предприятията трябва да положат всички усилия за спазване на насоките и препоръките.

83. Компетентните органи, които спазват или възнамеряват да спазват настоящите насоки, следва да ги включат по подходящ начин в своята регулаторна или надзорна рамка.

84. Компетентните органи трябва да потвърдят пред EIOPA дали спазват или възнамеряват да спазват настоящите насоки, като посочат причините за неспазване, в срок от два месеца от датата на публикуването на преводните версии.

85. При липса на отговор в този срок се счита, че компетентните органи не спазват изискването за докладване и това се докладва.

Заключителна разпоредба относно преразглежданията

86. Настоящите препоръки подлежат на преразглеждане от страна на EIOPA.