Насоки 01/2021

относно примерни случаи, свързани с уведомяването за нарушение на сигурността на личните данни

Приети на 14 декември 2021 г.

Версия 2.0

Приети — след обществена консултация

История на версиите

Версия 2.0	14.12.2021 г.	Приемане на насоките след обществена консултация
Версия 1.0	14.1.2021 г.	Приемане на насоките за обществена консултация

Съдържание

1 ВЪВЕДЕНИЕ 5

2 СОФТУЕР ЗА ИЗНУДВАНЕ 8

2.1 СЛУЧАЙ № 01: Софтуер за изнудване с подходящо архивиране и без ексфилтрация на данни 9

2.1.1 СЛУЧАЙ № 01 — Предварителни мерки и оценка на риска 9

2.1.2 СЛУЧАЙ № 01 — Смекчаване на последиците и задължения 10

2.2 СЛУЧАЙ № 02: Софтуер за изнудване без подходящо архивиране 11

2.2.1 СЛУЧАЙ № 02 — Предварителни мерки и оценка на риска 11

2.2.2 СЛУЧАЙ № 02 — Смекчаване на последиците и задължения 12

2.3 СЛУЧАЙ № 03: Случай в болница със софтуер за изнудване с резервно копие и без ексфилтрация 13

2.3.1 СЛУЧАЙ № 03 — Предварителни мерки и оценка на риска 13

2.3.2 СЛУЧАЙ № 03 — Смекчаване на последиците и задължения 14

2.4 СЛУЧАЙ № 04: Софтуер за изнудване без резервно копие и с ексфилтрация 14

2.4.1 СЛУЧАЙ № 04 — Предварителни мерки и оценка на риска 15

2.4.2 СЛУЧАЙ № 04 — Смекчаване на последиците и задължения 15

2.5 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от атаки със софтуер за изнудване 16

3 АТАКИ, ВКЛЮЧВАЩИ ЕКСФИЛТРАЦИЯ НА ДАННИ 17

3.1 СЛУЧАЙ № 05: Ексфилтрация от уебсайт на данни, свързани с кандидатстване за работно място 18

3.1.1 СЛУЧАЙ № 05 — Предварителни мерки и оценка на риска 18

3.1.2 СЛУЧАЙ № 05 — Смекчаване на последиците и задължения 19

3.2 СЛУЧАЙ № 06: Ексфилтрация на хеширана парола от уебсайт 19

3.2.1 СЛУЧАЙ № 06 — Предварителни мерки и оценка на риска 19

3.2.2 СЛУЧАЙ № 06 — Смекчаване на последиците и задължения 20

3.3 СЛУЧАЙ № 07: Атака с пълнене на идентификационни данни на банков уебсайт 21

3.3.1 СЛУЧАЙ № 07 — Предварителни мерки и оценка на риска 21

3.3.2 СЛУЧАЙ № 07 — Смекчаване на последиците и задължения 22

3.4 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от хакерски атаки 22

4 ВЪТРЕШЕН ИЗТОЧНИК НА РИСК, ПОРОДЕН ОТ РОЛЯТА НА ЧОВЕКА 23

4.1 СЛУЧАЙ № 08: Ексфилтрация на бизнес данни от служител 23

4.1.1 СЛУЧАЙ № 08 — Предварителни мерки и оценка на риска 23

4.1.2 СЛУЧАЙ № 08 — Смекчаване на последиците и задължения 24

4.2 СЛУЧАЙ № 09: Случайно предаване на данни към доверена трета страна 26

4.2.1 СЛУЧАЙ № 09 — Предварителни мерки и оценка на риска 26

4.2.2 СЛУЧАЙ № 09 — Смекчаване на последиците и задължения 26
4.3 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от вътрешните източници на риск, породен от ролята на човека 27
5 ИЗГУБЕНИ ИЛИ ОТКРАДНАТИ УСТРОЙСТВА И ДОКУМЕНТИ НА ХАРТИЯ 28
5.1 СЛУЧАЙ № 10: Откраднат материал, в който са се съхранявали криптирани лични данни 28
5.1.1 СЛУЧАЙ № 10 — Предварителни мерки и оценка на риска 28
5.1.2 СЛУЧАЙ № 10 — Смекчаване на последиците и задължения 29
5.2 СЛУЧАЙ № 11: Откраднат материал, в който са се съхранявали некриптирани лични данни 29
5.2.1 СЛУЧАЙ № 11 — Предварителни мерки и оценка на риска 29
5.2.2 СЛУЧАЙ № 11 — Смекчаване на последиците и задължения 30
5.3 СЛУЧАЙ № 12: Откраднати досиета на хартиен носител с чувствителни данни 30
5.3.1 СЛУЧАЙ № 12 — Предварителни мерки и оценка на риска 30
5.3.2 СЛУЧАЙ № 12 — Смекчаване на последиците и задължения 31
5.4 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от загубата или кражбата на устройства 31
6 ПОГРЕШНО ИЗПРАЩАНЕ НА ПОЩЕНСКА ПРАТКА 32
6.1 СЛУЧАЙ № 13: Грешка при изпращане на пощенска пратка 32
6.1.1 СЛУЧАЙ № 13 — Предварителни мерки и оценка на риска 32
6.1.2 СЛУЧАЙ № 13 — Смекчаване на последиците и задължения 32
6.2 СЛУЧАЙ № 14: Силно поверителни лични данни, изпратени по пощата по погрешка 33
6.2.1 СЛУЧАЙ № 14 — Предварителни мерки и оценка на риска 33
6.2.2 СЛУЧАЙ № 14 — Смекчаване на последиците и задължения 33
6.3 СЛУЧАЙ № 15: Лични данни, изпратени по пощата по погрешка 33
6.3.1 СЛУЧАЙ № 15 — Предварителни мерки и оценка на риска 34
6.3.2 СЛУЧАЙ № 15 — Смекчаване на последиците и задължения 34
6.4 СЛУЧАЙ № 16: Грешка при изпращане на пощенска пратка ... **Error! Bookmark not defined.**
6.4.1 СЛУЧАЙ № 16 — Предварителни мерки и оценка на риска 35
6.4.2 СЛУЧАЙ № 16 — Смекчаване на последиците и задължения 35
6.5 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от погрешно изпращане на пощенски пратки 35
7 Други случаи — социално инженерство 36
7.1 СЛУЧАЙ № 17: Кражба на самоличност 36
7.1.1 СЛУЧАЙ № 17 — Оценка на риска, смекчаване на последиците и задължения 37
7.2 СЛУЧАЙ № 18: Ексфилтрация по електронна поща 37
7.2.1 СЛУЧАЙ № 18 — Оценка на риска, смекчаване на последиците и задължения 38

ЕВРОПЕЙСКИЯТ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ,

като взе предвид член 70, параграф 1, буква д) от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за ЕИП, и по-специално приложение XI и Протокол 37 към него, изменени с Решение № 154/2018 на Съвместния комитет на ЕИП от 6 юли 2018 г.[1],

като взе предвид членове 12 и 22 от своя Правилник за дейността,

като взе предвид Съобщението на Комисията до Европейския Парламент и Съвета, озаглавено „Защитата на данните като стълб на оправомощаването на гражданите и подхода на ЕС по отношение на цифровия преход — две години от прилагането на Общия регламент относно защитата на данните“[2],

ПРИЕ СЛЕДНИТЕ НАСОКИ

1 ВЪВЕДЕНИЕ

1. С ОРЗД се въвежда в някои случаи изискването за уведомяване на компетентния национален надзорен орган (наричан по-долу „НО“) за нарушение на сигурността на личните данни и за съобщаване за нарушението на лицата, чиито лични данни са засегнати от него (членове 33 и 34).

2. През октомври 2017 г. Работната група за защита на личните данни по член 29 представи *общи* насоки относно уведомяването за нарушения на сигурността на личните данни, в които се анализират съответните раздели на ОРЗД („Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679“, РД 250) (наричани по-долу „Насоки на РД 250“)[3]. Поради естеството и момента на представяне на тези насоки, обаче, в тях не всички въпроси бяха разгледани достатъчно подробно. Ето защо се породи необходимостта от *практически указания, основани на конкретни случаи*, в които се използва опита, натрупан от НО след влизането в сила на ОРЗД.

[1] Позоваването на „държави членки“ в настоящия документ следва да се разбира като позоваване на „държавите — членки на ЕИП“.

[2] COM(2020) 264 final, 24 юни 2020 г.

[3] РГ 29 РД 250 rev.1, 6 февруари 2018 г., Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679, одобрени от ЕКЗД, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

3. Настоящият документ има за цел да допълни Насоките на РД 250, като в него са отразени сходните случаи, споделяни от НО от ЕИП след влизането в сила на ОРЗД. Целта е да се помогне на администраторите на лични данни да вземат решения как да се справят с нарушенията на сигурността на личните данни и какви фактори да вземат под внимание при оценката на риска.

4. Като част от всеки опит за предотвратяване на нарушение администраторът на лични данни и обработващият лични данни трябва първо да могат да го разпознаят. В член 4, параграф 12 от ОРЗД „нарушение на сигурността на личните данни“ е определено като „нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин“.

5. В своето Становище 03/2014 относно уведомяване за нарушаване[4] и в своите Насоки на РД 250 Работната група по член 29 пояснява, че нарушенията могат да бъдат категоризирани по следните три, добре известни принципа на информационната сигурност:

   - „Нарушение на поверителността“ — когато има неразрешено или случайно разкриване или достъп до лични данни.
   - „Нарушение на целостта“ — когато има неразрешена или случайна промяна на лични данни.
   - „Нарушение на наличността“ — когато има неразрешена или случайна загуба на достъп до или унищожаване на лични данни.[5]

6. Нарушението може евентуално да предизвика редица значителни неблагоприятни последици за физическите лица, които може да породят физически, материални или нематериални вреди. В ОРЗД се пояснява, че това може да включва загуба на контрол върху личните им данни, ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизация, накърняване на репутацията и нарушаване на поверителността на лични данни, защитени от професионална тайна. Това може да включва и всякакви други значителни икономически или социални неблагоприятни последствия за тези физически лица. Едно от най-важните задължения на администратора на лични данни е да направи оценка на тези рискове за правата и свободите на субектите на данни и да приложи подходящи технически и организационни мерки, необходими за тяхното преодоляване.

7. Съответно в ОРЗД е предвидено изискване администраторът да:

   - документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него[6];

---

[4] РГ 29 РД 213, 25 март 2014 г., Становище 03/2014 относно уведомяване за нарушение на сигурността на личните данни, стр. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4 .

[5] Вж. Насоките на РД 250, стр. 7. — Трябва да се има предвид, че нарушение на сигурността на данните може да засяга една категория или повече категории едновременно или комбинация от тях.

[6] Член 33, параграф 5 от ОРЗД.

- уведомява за нарушението на сигурността на личните данни надзорния орган, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица[7];
- съобщава на субекта на данните за нарушението на сигурността на личните данни, когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица[8].

8. Нарушенията на сигурността на данните представляват проблеми сами по себе си, но могат да бъдат и симптоми на уязвим, вероятно остарял режим за сигурност на данните, както могат и да показват слабости на системата, които трябва да бъдат отстранени. Като общо правило винаги е по-добре да се предотвратят нарушенията на сигурността на данните чрез добра предварителна подготовка, тъй като някои последици от тях са необратими по своето естество. Преди администраторът да може да направи *пълна* оценка на риска, произтичащ от нарушение, причинено от някакъв вид атака, следва да бъде определена първопричината, за да се установи дали все още са налице уязвимостите, довели до инцидента, и следователно дали все още осигуряват възможност за атака. В много случаи администраторът може да установи, че има вероятност инцидентът да доведе до риск, и следователно за него трябва да бъде изпратено уведомление. В други случаи не е необходимо уведомлението да се отлага, докато за риска и въздействието на нарушението бъде изготвена пълна оценка, тъй като пълната оценка на риска може да се извърши успоредно с уведомлението и така получената информация може да бъде предоставена на НО на етапи без ненужно допълнително забавяне[9].

9. За нарушението следва да бъде изпратено уведомление, когато администраторът е на мнение, че има вероятност то да породи риск за правата и свободите на субекта на данни. Администраторите следва да изготвят тази оценка в момента, в който разберат за нарушението. Администраторът не трябва да чака изготвянето на подробна съдебно-техническа експертиза и предприемането на (предварителни) стъпки за смекчаване, преди да направи оценка дали нарушението на сигурността на личните данни има вероятност да породи риск и поради това следва да бъде изпратено уведомление.

10. Ако администраторът сам прецени, че вероятността за риска е малка, но въпреки това рискът се материализира, компетентният НО може да използва своите корективни правомощия и да вземе решение за налагане на санкции.

11. Всички администратори и обработващи лични данни следва да имат разработени планове и процедури за справяне с евентуални нарушения на сигурността на личните данни. Организациите трябва да имат ясни процедури за отчитане и отговорни лица за определени аспекти на процеса за възстановяване.

12. От съществено значение за администраторите и обработващите лични данни също е обучението и информираността на персонала на администратора и на обработващия лични данни по въпросите, свързани със защитата на личните данни, с акцент върху управлението на нарушенията на сигурността на личните данни (установяване на случай на нарушение на сигурността на личните

[7] Член 33, параграф 1 от ОРЗД.

[8] Член 34, параграф 1 от ОРЗД.

[9] Член 33, параграф 4 от ОРЗД.

данни, допълнителни действия, които трябва да бъдат предприети, и др.). Това обучение следва да бъде провеждано през определен период от време, в зависимост от вида на дейността по обработването и размера на администратора, като се вземат предвид най-новите тенденции и сигнали, произтичащи от кибератаки или други инциденти в областта на киберсигурността.

13. Принципът на отчетност и концепцията за защита на данните на етапа на проектирането биха могли да включват анализ, който да се използва в собствения „Наръчник за реакция при нарушения на сигурността на личните данни“ на администратора на лични данни и на обработващия лични данни, който има за цел да се установят фактите за всеки аспект от обработването на всеки основен етап от дейността. Такъв предварително разработен наръчник би осигурил много по-бърз източник на информация, който да даде възможност на администраторите на лични данни и на обработващите да намалят рисковете и да изпълнят задълженията си без ненужно забавяне. По този начин би се гарантирало, че ако възникне нарушение на сигурността на личните данни, хората в организацията ще знаят какво да правят и има голяма вероятност инцидентът да бъде разгледан по-бързо, отколкото ако няма въведени смекчаващи мерки или план.

14. Въпреки че представените по-долу случаи са фиктивни, те се основават на типични случаи от колективния опит на надзорните органи с уведомления за нарушения на сигурността на личните данни. Предлаганите анализи се отнасят изрично до разглежданите случаи, но с цел да осигурят съдействие на администраторите на лични данни при оценката на собствените им нарушения на сигурността на личните данни. Всяка промяна в обстоятелствата на описаните по-долу случаи може да доведе до различни или по-високи нива на риск, като следователно ще бъде необходимо да се предприемат различни или допълнителни мерки. В тези насоки случаите са структурирани по определени категории нарушения (например атаки със софтуер за изнудване). Във всеки отделен случай са необходими определени мерки за смекчаване на риска, когато се работи с определени категории нарушения. Тези мерки не се повтарят непременно във всеки анализ на отделен случай, принадлежащ към определена категория нарушения. За случаите, принадлежащи към една и съща категория, се описват само разликите. Ето защо читателят следва да прочете всички случаи, които се отнасят до определена категория нарушение, за да установи и разграничи всички подходящи мерки, които могат да бъдат предприети.

15. Вътрешното документиране на дадено нарушение е задължение, което не е обвързано с рисковете, свързани с нарушението, и трябва да се извършва във всеки отделен случай. С представените по-долу случаи се прави опит да се изясни дали за дадено нарушение трябва да се изпрати уведомление до НО и да се съобщи на засегнатите субекти на данни.

2 СОФТУЕР ЗА ИЗНУДВАНЕ

16. Честа причина за уведомяване за нарушение на сигурността на личните данни е атака със софтуер за изнудване, претърпяна от администратор на лични данни. В тези случаи зловреден код криптира личните данни и впоследствие атакуващият иска от администратора откуп в замяна на кода за декриптиране. Този вид атака обикновено може да се класифицира като нарушение на наличността, но често може да възникне и нарушение на поверителността.

2.1 СЛУЧАЙ № 01: Софтуер за изнудване с подходящо архивиране и без ексфилтрация на данни

Компютърните системи на малко производствено дружество са атакувани със софтуер за изнудване и данните, съхранявани в тези системи, са криптирани. Администраторът на лични данни е използвал криптиране в покой, така че всички данни, до които е осъществен достъп със софтуера за изнудване, са се съхранявали в криптирана форма с помощта на съвременен алгоритъм за криптиране. По време на атаката не е компрометиран ключът за декриптиране, т.е. атакуващият не е успял нито да получи достъп до него, нито да го използва непряко. В резултат на това атакуващият е имал достъп само до криптирани лични данни. По-конкретно, нито системата за електронна поща на дружеството, нито клиентските системи, използвани за достъп до нея, са били засегнати. Дружеството използва експертния опит на външно дружество в областта на киберсигурността, за да обследва инцидента. На разположение са регистри, проследяващи всички потоци от данни, напускащи дружеството (в това число и изходяща електронна поща). След анализ на регистрите и данните, събрани от внедрените от дружеството системи за откриване, вътрешно разследване, подпомогнато от външното дружество в областта на киберсигурността, разкрива *със сигурност*, че извършителят само е криптирал данни, без да ги изнесе. Според информацията в регистрите няма изходящ поток от данни във времевата рамка на атаката. Личните данни, засегнати от нарушението, са свързани с клиенти и служители на дружеството, общо няколко десетки лица. На разположение е лесно достъпно резервно копие и данните са възстановени няколко часа след атаката. Нарушението не е довело до никакви последици за ежедневната дейност на администратора. Не е имало забавяне при плащанията на служителите или обработката на заявки на клиенти.

17. В този случай са реализирани следните елементи от определението за „нарушение на сигурността на личните данни“: нарушение на сигурността е довело до незаконна промяна и неразрешен достъп до съхраняваните лични данни.

2.1.1 СЛУЧАЙ № 01 — Предварителни мерки и оценка на риска

18. По аналогия с всички рискове, породени от външни участници, вероятността атаката със софтуер за изнудване да бъде успешна може да бъде драстично намалена чрез засилване на сигурността на средата за контрол на данните. По-голямата част от тези нарушения могат да бъдат предотвратени, като се гарантира, че са взети подходящи организационни, физически и технологични мерки за сигурност. Примери за такива мерки са правилното управление на корекции и използването на подходяща система за откриване и отстраняване на зловреден софтуер. Наличието на подходящо отделно резервно копие ще спомогне за смекчаване на последиците от атаката, ако такава бъде успешно извършена. Освен това програма за образование, обучение и информираност на служителите в областта на сигурността (SETA) ще помогне за предотвратяване и разпознаване на този вид атаки. (Списък с препоръчителни мерки може да бъде намерен в раздел 2.5) Тъй като по-голямата част от атаките със софтуер за изнудване се възползват от добре известни уязвимости, една от най-важните сред тези мерки е правилното управление на корекциите, с което се гарантира, че системите са актуализирани и всички известни уязвимости на внедрените системи са поправени.

19. При оценката на рисковете администраторът следва да обследва нарушението и да идентифицира типа на зловредния код, за да разбере възможните последици от атаката. Сред рисковете, които трябва да се предвидят, е рискът данните да са били изнесени, без да е останала следа за това в регистрите на системите.

20. В този пример атакуващият е имал достъп до лични данни и е компрометирана поверителността на текста на шифъра, съдържащ лични данни в криптирана форма. Въпреки това данните, които може да са били

изнесени, не могат да бъдат прочетени или използвани от извършителя, поне за момента. Техниката за криптиране на данни, използвана от администратора на данни, отговаря на съвременното технологично равнище. Ключът за декриптиране не е компрометиран и вероятно също не е можело да бъде определен с други средства. Вследствие на това свързаните с поверителността рискове за правата и свободите на физическите лица са намалени до минимум, което не позволява да се постигне напредък по отношение на криптоанализа, който в бъдещ момент прави разбираеми криптираните данни.

21. Администраторът на лични данни следва да вземе предвид риска за физическите лица поради нарушението[10]. В този случай изглежда, че рисковете за правата и свободите на субектите на данни произлизат от това, че личните данни не са налични, и поверителността на личните данни не е компрометирана[11]. В този пример, неблагоприятните последици са смекчени сравнително скоро след извършването на нарушението. Наличието на подходящ режим за архивиране[12] прави последиците по-малко сериозни и тук администраторът успява да го използва ефективно.

22. По отношение на тежестта на последиците за субектите на данни беше установен само незначителен ефект, тъй като засегнатите данни бяха възстановени само след няколко часа, нарушението не оказа никакво въздействие върху ежедневната работа на администратора и нямаше сериозно влияние върху субектите на данни (например- плащанията на служителите или обработката на заявки на клиенти).

2.1.2 СЛУЧАЙ № 01 — Смекчаване на последиците и задължения

23. Без резервно копие администраторът може да предприеме само няколко мерки за възстановяване на загубата на лични данни, като данните трябва да бъдат събрани отново. В този конкретен случай обаче въздействието от атаката можеше да бъде ограничено ефективно чрез нулиране на всички компрометирани системи до чисто състояние, за което се знае, че няма зловреден код, отстраняване на уязвимостите и възстановяване на засегнатите данни скоро след атаката. Без резервно копие данните се загубват и сериозността може да се увеличи, защото рисковете за физическите лица или въздействията върху тях също могат да бъдат по-големи.

---

[10] За насоки относно операциите по обработване, за които *„съществува вероятност да породят висок риск“*, вж. Насоките на Работната група по член 29 относно оценката на въздействието върху защитата на данните (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679, РД 248 ред.01 — одобрени от ЕКЗД,https://ec.europa.eu/newsroom/article29/items/611236, стр. 9.

[11] От техническа гледна точка криптирането на данни ще включва „достъп“ до оригинални данни, а в случая на софтуер за изнудване, изтриването на оригинала — до данните трябва да бъде осъществен достъп от код на софтуер за изнудване, за да ги криптира и да премахне оригиналните данни. Атакуващият може да направи копие на оригинала преди изтриването, но личните данни не винаги могат да бъдат извлечени. С напредването на разследването на администратора на данни може да се появи нова информация, което да промени оценката. Достъпът, който води до неправомерно унищожаване, загуба, промяна, неразрешено разкриване на личните данни или до риск за сигурността на субект на данни, дори без тълкуване на данните може да бъде също толкова сериозен като достъпа с тълкуване на личните данни.

[12] Процедурите за архивиране следва да бъдат структурирани, последователни и повтарящи се. Примери за процедури за архивиране са методът 3-2-1 и методът дядо-баща-син. Всеки метод следва винаги да се тества за ефективност на покритието и кога данните трябва да бъдат възстановени. Тестването също следва да се повтаря на интервали и особено когато настъпят промени в операцията по обработване или нейните обстоятелства, за да се гарантира целостта на системата.

24. Навременното ефективно възстановяване на данни от леснодостъпното резервно копие е ключова променлива величина, когато се анализира нарушението. Определянето на подходящ график за възстановяване на компрометираните данни зависи от конкретните обстоятелства на разглежданото нарушение. В ОРЗД се посочва, че за нарушение на сигурността на личните данни се изпраща уведомление без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа. Ето защо може да се определи, че при всички случаи не се препоръчва надхвърлянето на срока от 72 часа, но когато случаят поражда висок риск, дори спазването на този срок може да се разглежда като незадоволително.

25. В този случай, след подробна оценка на въздействието и процедура за реагиране при инциденти, администраторът определи, че е малко вероятно нарушението да доведе до риск за правата и свободите на физическите лица, поради което не е необходимо да се изпраща съобщение до субектите на данни, както и не се налага изпращане на уведомление относно нарушението до надзорния орган. Както всяко нарушение на сигурността на личните данни обаче то следва да бъде документирано в съответствие с член 33, параграф 5. Може също така да се наложи (или на по-късен етап да бъде изискано от НО) организацията да актуализира и да отстрани недостатъците в своите организационни и технически мерки и процедури за управление на сигурността на личните данни, и за намаляване на риска. В рамките на този етап на актуализиране и отстраняване на недостатъците организацията следва задълбочено да разследва нарушението и да установи причините и методите, използвани от извършителя, за да предотврати подобни събития в бъдеще.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	X	X

2.2 СЛУЧАЙ № 02: Софтуер за изнудване без подходящо архивиране

Един от компютрите, използвани от селскостопанско дружество, е атакувано със софтуер за изнудване, а неговите данни са криптирани от атакуващия. Дружеството използва експертния опит на външна фирма в областта на киберсигурността, за да наблюдава неговата мрежа. На разположение са регистри, проследяващи всички потоци от данни, напускащи дружеството (в това число и изходяща електронна поща). След анализ на регистрите и данните, събрани от другите системи за откриване, вътрешното разследване, подпомогнато от дружеството в областта на киберсигурността, разкрива, че извършителят само е криптирал данните, без да ги изнесе. Според информацията в регистрите няма изходящ поток от данни във времевата рамка на атаката. Личните данни, засегнати от нарушението, са свързани със служителите и клиентите на дружеството, общо няколко десетки лица. Не са засегнати специални категории лични данни. Не е имало резервно копие в електронна форма. По-голямата част от данните са възстановени от архиви на хартиен носител. Възстановяването на данните отне 5 работни дни и доведе до минимално забавяне на доставките на поръчки на клиентите.

2.2.1 СЛУЧАЙ № 02 — Предварителни мерки и оценка на риска

26. Администраторът на лични данни следва да е въвел същите предварителни мерки, като посочените в част 2.1. и раздел 2.9. Основната разлика с предишния случай е липсата на електронен архив и липсата на криптиране в покой. Това води до фундаментални разлики в следващите стъпки.

27. При оценката на рисковете администраторът следва да обследва метода на проникване и да идентифицира типа на зловредния код, за да разбере възможните последици от атаката. В този пример софтуерът за изнудване криптира личните данни, без да ги изнася. В резултат на това изглежда, че рисковете за правата и свободите на субектите на данни произлизат от това, че личните данни не са

налични, и поверителността на личните данни не е компрометирана. От изключителна важност за определяне на риска е да се извърши задълбочено проучване на регистрите на защитната стена и на тяхното значение. При поискване администраторът на лични данни следва да представи фактите, установени при тези обследвания.

28. Администраторът на лични данни трябва да има предвид, че ако атаката е по-сложна, софтуерът за изнудване има функцията да редактира регистрационните файлове и да изтрива следата. Така че, предвид факта, че записите не се препращат или репликират в сървър на централен системен регистър, дори след като задълбоченото разследване е установило, че личните данни не са извлечени от атакуващия, администраторът на лични данни не може да твърди, че липсата на запис в регистъра доказва, че не е направено извличане, и поради това не може напълно да се отхвърля вероятността за нарушение на поверителността.

29. Ако атакуващият е осъществил достъп до данните, администраторът на лични данни следва да направи оценка на рисковете, произтичащи от това нарушение[13]. При оценката на риска администраторът следва да вземе под внимание естеството, чувствителността, обема и контекста на личните данни, засегнати от нарушението. В този случай не са засегнати специални категории лични данни, а количеството на засегнатите данни и броят на засегнатите субекти на лични данни са малки.

30. Събирането на точна информация за неразрешения достъп е от ключово значение за определяне на нивото на риск и за предотвратяване на нова атака или на продължаваща атака. Ако данните са били копирани от базата данни, това очевидно би било фактор, който увеличава риска. Когато липсва сигурност по отношение на спецификата на незаконния достъп, следва да се разгледа по-лошият сценарий и да се направи съответната оценка на риска.

31. Липсата на резервна база данни може да се разглежда като фактор, който увеличава риска, в зависимост от тежестта на последиците за субектите на данни, произлизащи от липсата на налични данни.

2.2.2 СЛУЧАЙ № 02 — Смекчаване на последиците и задължения

32. Без резервно копие администраторът може да предприеме само няколко мерки за възстановяване на загубата на лични данни, като данните трябва да бъдат събрани отново, освен ако не е наличен друг източник (например- електронни писма за потвърждение на поръчки). Без резервно копие данните могат да бъдат загубени, а сериозността ще зависи от въздействието върху физическите лица.

33. Възстановяването на данните не следва да бъде прекалено трудно[14], ако данните са налични и на хартиен носител, но като се има предвид липсата на електронна резервна база данни, се счита за необходимо да се изпрати уведомление до НО, тъй като възстановяването на данните е отнело известно време и би могло да доведе до забавяния в доставката на поръчките на клиентите и има вероятност сериозно количество метаданни (например регистри, времеви печати) да не може да бъде възстановено.

---

[13] За насоки относно операциите по обработване, за които „*съществува вероятност да породят висок риск*“, вж. бележка под линия 10 по-горе.

[14] Това ще зависи от сложността и структурата на личните данни. В най-сложните сценарии има вероятност да са необходими значителни ресурси и усилия за възстановяване на целостта на данните, съгласуваност с метаданните, осигуряване на правилните връзки в рамките на структурите на данните и проверяване на точността на данните.

34. Информирането на субектите на данни за нарушението може да зависи също от продължителността на периода, през който личните данни не са налични, и от трудностите, които това може да причини за работата на администратора (например- забавяния на плащанията на служителите). Тъй като забавянията на плащанията и на доставките може да доведе до финансови загуби за физическите лица, чиито данни са били компрометирани, може да се твърди също, че има вероятност нарушението да доведе до висок риск. Също така има вероятност информирането на субектите на данни да не може да се избегне, когато те трябва да предоставят информация, необходима за възстановяване на криптираните данни.

35. Този случай служи като пример за атака със софтуер за изнудване, пораждаща риск за правата и свободите на субектите на данни, но която не достига висок риск. Тя следва да бъде документирана в съответствие с член 33, параграф 5, а уведомление за нея следва да бъде изпратено до НО в съответствие с член 33, параграф 1. Може също така да се наложи (или да бъде изискано от НО) организацията да актуализира и да отстрани недостатъците в своите организационни и технически мерки и процедури за управление на сигурността на личните данни и за намаляване на риска.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	X

2.3 СЛУЧАЙ № 03: Случай в болница със софтуер за изнудване с резервно копие и без ексфилтрация

Информационната система на болница/център за здравно обслужване е атакувана със софтуер за изнудване и значителна част от данните в нея са криптирани от атакуващия. Дружеството използва експертния опит на външна фирма в областта на киберсигурността, за да наблюдава неговата мрежа. На разположение са регистри, проследяващи всички потоци от данни, напускащи дружеството (в това число и изходяща електронна поща). След анализ на регистрите и данните, събрани от другите системи за откриване, вътрешното разследване, подпомогнато от дружеството в областта на киберсигурността, разкрива, че извършителят само е криптирал данните, без да ги изнесе. Според информацията в регистрите няма изходящ поток от данни във времевата рамка на атаката. Личните данни, засегнати от нарушението, са свързани със служителите и пациентите, което представлява хиляди физически лица. Налични са били резервни копия в електронна форма. По-голямата част от данните са възстановени, но тази операция е продължила 2 работни дни и е довела до големи забавяния в лечението на пациентите с отменена/отложена операция, както и до намаляване на нивото на обслужване поради това, че системите не са били налични.

2.3.1 СЛУЧАЙ № 03 — Предварителни мерки и оценка на риска

36. Администраторът на лични данни следва да е въвел същите предварителни мерки, като посочените в част 2.1. и раздел 2.5. Основната разлика с предишния случай е голямата сериозност на последиците за значителна част от субектите на данни[15].

[15] За насоки относно операциите по обработване, за които *„съществува вероятност да породят висок риск“*, вж. бележка под линия 10 по-горе.

37. Количеството на засегнатите данни и броят на засегнатите субекти на лични данни са високи, тъй като болниците обикновено обработват огромни количества данни. Липсата на достъпност на данните има голямо въздействие върху значителна част от субектите на данни. Освен това съществува и остатъчен риск от много сериозни последици за поверителността на данните на пациентите.

38. Важни са видът на нарушението, естеството, чувствителността и обемът на личните данни, засегнати от нарушението. Въпреки че е имало резервно копие на данните и то е можело да бъде възстановено за няколко дни, все пак съществува висок риск поради сериозността на последиците за субектите на данни, произтичащи от липсата на налични данни в момента на атаката и през следващите дни.

2.3.2 СЛУЧАЙ № 03 — Смекчаване на последиците и задължения

39. Счита се, че е необходимо НО да бъде уведомен, тъй като са замесени специални категории лични данни и възстановяването на данните би могло да отнеме дълго време, което ще доведе до големи забавяния в грижите за пациентите. Поради въздействието върху пациентите е необходимо за нарушението да бъдат информирани и субектите на данни, дори след възстановяване на криптираните данни. Макар че данните, свързани с всички пациенти, лекувани в болницата през последните години, са криптирани, само пациентите, за които е било планирано да бъдат лекувани в болницата в момента, когато компютърната система е била недостъпна, са засегнати. Администраторът следва пряко да съобщи на тези пациенти за нарушението на сигурността на личните данни. Осъществяването на пряка комуникация с другите пациенти, някои от които има вероятност да не са били в болницата повече от двадесет години, може да не се изисква поради изключението, предвидено в член 34, параграф 3, буква в). В такъв случай се прави публично съобщение[16] или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани. В този случай болницата следва да оповести публично атаката със софтуер за изнудване и нейните последици.

40. Този случай служи като пример за атака със софтуер за изнудване, пораждаща висок риск за правата и свободите на субектите на данни. Тя следва да бъде документирана в съответствие с член 33, параграф 5, уведомление за нея следва да бъде изпратено до НО в съответствие с член 33, параграф 1, както и да бъде изпратено съобщение за нея до субектите на данни в съответствие с член 34, параграф 1. Организацията също така трябва да актуализира и да отстрани недостатъците в своите организационни и технически мерки и процедури за управление на сигурността на личните данни и за намаляване на риска.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	✓

2.4 СЛУЧАЙ № 04: Софтуер за изнудване без резервно копие и с ексфилтрация

[16] В съображение 86 от ОРДЗ е обяснено, че „*такива уведомления до субектите на данни следва да бъдат правени веднага щом това е разумно осъществимо и в тясно сътрудничество с надзорния орган, като се спазват насоките, предоставени от него или от други съответни органи, като правоприлагащите органи. Така например необходимостта да се ограничи непосредственият риск от вреди би наложила незабавното уведомяване на субектите на данните, докато необходимостта от предприемането на целесъобразни мерки срещу продължаването на нарушения на сигурността на личните данни или срещу подобни нарушения би оправдало по-дълги срокове за уведомлението*.“

Сървърът на дружество за обществен транспорт е атакуван със софтуер за изнудване, а данните на него са криптирани от атакуващия. Вътрешното разследване установява, че извършителят не само е криптирал данните, но също така ги е изнесъл. Данните, попадащи в обхвата на нарушението, са личните данни на клиенти и служители, както и на няколко хиляди човека, които използват услугите на дружеството (например купуват билети онлайн). Не само основни данни за самоличност, но и номера на лични карти и финансови данни, като данните от кредитни карти, са замесени в нарушението. Съществувала е резервна база данни, но тя също е била криптирана от атакуващия.

2.4.1 СЛУЧАЙ № 04 — Предварителни мерки и оценка на риска

41. Администраторът на лични данни следва да е въвел същите предварителни мерки, като посочените в част 2.1. и раздел 2.5. Въпреки че е съществувало резервно копие, то също е засегнато от атаката. Тази конфигурация сама по себе си повдига въпроси за качеството на предишните мерки на администратора за сигурност на ИТ и следва да бъде допълнително проверена по време на разследването, тъй като в един добре проектиран режим за архивиране трябва да се съхраняват множество резервни копия по сигурен начин без достъп от основната система, в противен случай те могат да бъдат компрометирани при същата атака. Освен това атаките със софтуер за изнудване могат да останат неразкрити дни наред, като бавно криптират рядко използвани данни. Това може да направи множеството резервни копия неизползваеми, ето защо резервни копия също следва да се правят периодично и да се изолират. Това би увеличило вероятността за възстановяване, макар и с по-голяма загуба на данни.

42. Това нарушение засяга не само наличността на данните, но също така и поверителността, тъй като има вероятност атакуващият да е променил и/или копирал данни от сървъра. Следователно видът на нарушението поражда висок риск[17].

43. Естеството, чувствителността и обемът на личните данни допълнително повишават риска, тъй като броят на засегнатите физически лица е висок, като същото се отнася и за общото количество засегнати лични данни. Замесени са не само основни данни за самоличност, но и документи за самоличност и финансови данни, като данните от кредитни карти. Нарушение на сигурността на личните данни във връзка с тези видове данни представлява висок риск само по себе си и ако се обработват заедно, те биха могли да се използват за кражба на самоличност или измама, наред с другото.

44. Поради погрешна логика на сървъра или поради неправилно организационно управление, резервните копия са засегнати от софтуера за изнудване, предотвратявайки възстановяването на данните и увеличавайки риска.

45. Това нарушение на сигурността на личните данни поражда висок риск за правата и свободите на физическите лица, тъй като има вероятност да доведе както до имуществени (например финансови загуби, тъй като са засегнати данни от кредитни карти), така и до неимуществени вреди (например кражба на самоличност или измама, тъй като са засегнати данни от лични карти).

2.4.2 СЛУЧАЙ № 04 — Смекчаване на последиците и задължения

46. Съобщаването на субектите на данните е особено важно, за да могат те да предприемат необходимите стъпки за предотвратяване на имуществени вреди (например да блокират своите кредитни карти).

[17] За насоки относно операциите по обработване, за които *„съществува вероятност да породят висок риск“*, вж. бележка под линия 10 по-горе.

47. Освен документиране на нарушението в съответствие с член 33, параграф 5, в този случай е задължително да бъде изпратено уведомление до надзорния орган (член 33, параграф 1), а администраторът е задължен също така да съобщи на субектите на данни за нарушението (член 34, параграф 1). Последното може да се извърши на индивидуална основа, но за физическите лица, чиито данни за връзка не са налични, администраторът следва да направи това публично, стига това съобщение да не предизвика допълнителни отрицателни последици за субектите на данни, например чрез публикуване на уведомление на своя уебсайт. В последния случай се изисква точно и ясно съобщение на видимо място на страницата на администратора, с точно позоваване на съответните разпоредби от ОРЗД. Може също да се наложи организацията да актуализира и да отстрани недостатъците в своите организационни и технически мерки и процедури за управление на сигурността на личните данни, и за намаляване на риска.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	✓

2.5 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от атаки със софтуер за изнудване

48. Фактът, че е можело да бъде извършена атака със софтуер за изнудване обикновено е признак за наличието на една или повече уязвимости в системата на администратора. Това се отнася и за случаите на атака със софтуер за изнудване, при които личните данни са били криптирани, но не и ексфилтрирани. Независимо от резултатите и последиците от атаката, силно се подчертава важността на извършването на всеобхватна оценка на системата за сигурност на данните, със специален акцент върху сигурността на ИТ. Установените слабости и пропуски в сигурността трябва да се документират и отстранят незабавно.

49. Препоръчителни мерки:

(Списъкът със следващите мерки в никакъв случай не е изключителен или изчерпателен. Целта е да се предложат идеи за превенция и възможни решения. Всяка дейност по обработване е различна, поради което администраторът следва да вземе решение кои мерки най-добре пасват на дадената ситуация.)

- Актуализиране на софтуера на производителя, операционната система и приложния софтуер на сървърите, клиентските машини, активните мрежови компоненти и друго оборудване на същата локална мрежа (включително Wi-Fi устройства). Въвеждане на подходящи мерки за сигурност на ИТ, гарантиране, че те са ефективни, и редовното им актуализиране, когато се променя или развива обработването или обстоятелствата. Това включва поддържане на подробни записи за това какви корекции са прилагани на кои времеви отпечатъци.
- Проектиране и организиране на системи за обработка и на инфраструктура за сегментиране или изолиране на системи и мрежи от данни, за да се предотврати размножаването на зловреден софтуер в рамките на организацията и неговото разпространение към външни системи.
- Наличие на актуална, сигурна и изпитана процедура за архивиране. Средствата за средносрочно и дългосрочно архивиране следва да се съхраняват отделно от оперативните средства за съхранение на данни и извън обсега на трети страни, дори в случай на успешна атака (като ежедневно поетапно архивиране и седмично пълно архивиране).
- Наличие/придобиване на подходящ, актуален, ефективен и интегриран софтуер за защита срещу зловреден софтуер.

- Наличие на подходяща, актуална, ефективна и интегрирана защитна стена и на система за установяване и предотвратяване на проникване. Насочване на мрежовия трафик през защитната стена/системата за установяване на проникване, дори в случаите на домашен офис или мобилна работа (например с използване на VPN връзки към организационните механизми за сигурност при достъп до интернет).
- Обучаване на служителите за методите на разпознаване и предотвратяване на атаки срещу информационните технологии. Администраторът следва да осигури средства за установяване на автентичността и надеждността на съобщенията по електронната поща и на съобщенията, получени чрез други средства за комуникация. Служителите следва да бъдат обучени да разпознават кога се е случила такава атака, как да извадят крайната точка от мрежата, както и за тяхното задължение незабавно да подадат сигнал за нея на служителя по сигурността.
- Подчертаване на необходимостта от идентифициране на вида на зловредния код, за да се разберат последиците от атаката и да могат да се намерят правилните мерки за смекчаване на риска. В случай че атаката със софтуер за изнудване е била успешна и няма налично резервно копие, за възстановяване на данните могат да се използват наличните инструменти, като тези от проекта „no more ransom“ [„стоп на изнудването“] (nomoreransom.org). В случай обаче, че има налично безопасно резервно копие, се препоръчва данните да бъдат възстановени от него.
- Насочване или репликиране на всички регистри към сървър на централен системен регистър (евентуално с подписване или криптографско добавяне на времеви печат на записите в регистъра).
- Сложно криптиране и многофакторно удостоверяване, по-специално за административния достъп до ИТ системите, подходящо управление на ключовете и паролите.
- Периодично изпитване за уязвимости и пробив.
- Създаване на екип за реагиране при инциденти с компютърната сигурност (CSIRT) или на екип за незабавно реагиране при компютърни инциденти (CERT) в рамките на организацията или присъединяване към колективен CSIRT/CERT. Създаване на план за реагиране при инциденти, на план за преодоляване на последствията от аварийна ситуация и на план за непрекъснатост на работата, както и задълбочено тестване на тези планове.
- При оценяването на мерките за противодействие следва да се прегледа, провери и актуализира анализът на риска.

3 АТАКИ, ВКЛЮЧВАЩИ ЕКСФИЛТРАЦИЯ НА ДАННИ

50. Атаките, които използват уязвимости на услугите, предлагани от администратора на трети страни по интернет, например извършени посредством атаки с инжектиране (например SQL инжектиране, обход на директория), компрометиране на уебсайт и други подобни методи, могат да наподобяват атаки със софтуер за изнудване по това, че рискът произлиза от действието на неоправомощена трета страна, но тези атаки обикновено имат за цел да копират, изнасят и злоупотребят с лични данни с някаква злонамерена цел. Ето защо те представляват предимно нарушения на поверителността, както и евентуално на целостта на данните. В същото време, ако администраторът е запознат с характеристиките на този вид нарушения, на разположение на администраторите има множество мерки, които могат съществено да намалят риска от успешно изпълнение на атака.

3.1 СЛУЧАЙ № 05: Ексфилтрация от уебсайт на данни, свързани с кандидатстване за работно място

Агенция за подбор на персонал става жертва на кибератака, която поставя зловреден код на нейния уебсайт. Този зловреден код прави личната информация, подадена чрез онлайн формуляри за кандидатстване за работа и съхранявана на уебсайта, достъпна за неоправомощени лица. Най-вероятно са засегнати 213 такива формуляри, като след анализ на засегнатите данни е установено, че при нарушението не са засегнати специални категории лични данни. Конкретният инсталиран зловреден набор от инструменти е имал функционалности, които са дали възможност атакуващият да премахне историята на извличането, както и е позволил обработката на сървъра да бъде наблюдавана и да бъдат иззети личните данни. Този набор от инструменти е открит чак един месец след неговото инсталиране.

3.1.1 СЛУЧАЙ № 05 — Предварителни мерки и оценка на риска

51. Сигурността на средата на администратора на лични данни е изключително важна, тъй като по-голямата част от нарушенията могат да бъдат избегнати, като се предприемат стъпки всички системи да бъдат постоянно актуализирани, чувствителните данни — криптирани, а приложенията — разработвани в съответствие с високи стандарти за сигурност, като надеждни методи за удостоверяване на автентичността, мерки срещу атаки с груба сила, „избягване“ или „цензуриране“[18] на информацията, въведена от потребителите, и др. Периодични проверки на сигурността на ИТ, оценки на уязвимостта и изпитвания за пробив също са необходими, за да могат тези видове уязвимости да се откриват предварително и да се отстраняват. В конкретния случай има вероятност инструментите за наблюдение на целостта на файловете в производствена среда да са помогнали за откриването на инжектирането на кода. (Списък с препоръчителни мерки може да бъде намерен в раздел 3.7)

52. Администраторът следва винаги да започва разследването на нарушението с идентифициране на вида на атаката и на нейните методи, за да оцени какви мерки трябва да бъдат предприети. За да го направи бързо и ефективно, администраторът на лични данни следва да разполага с план за реагиране при инциденти, в който са определени бързите и необходими стъпки за поемане на контрол над инцидента. В конкретния случай видът на нарушението е фактор, който увеличава риска, тъй като не само че поверителността на данните е ограничена, но и лицето, извършващо незаконното проникване, е разполагало със средствата да направи промени в системата, поради което целостта на данните също е поставена под въпрос.

53. Следва да се направи оценка на естеството, чувствителността и обема на личните данни, засегнати от нарушението, за да се определи до каква степен то е засегнало субектите на данни. Въпреки че не са засегнати специални категории лични данни, данните, до които е осъществен достъп, съдържат значителна информация за физическите лица от онлайн формулярите, а с такива данни може да се злоупотреби по няколко начина (получаване на нежелани рекламни съобщения, кражба на самоличност и т.н.), така че сериозността на последиците следва да увеличи риска за правата и свободите на субектите на данни[19].

[18] Избягването или цензурирането на информацията, въведена от потребителите, представлява форма на валидиране на въведената информация, което гарантира, че само правилно форматирани данни се въвеждат в дадена информационна система.

[19] За насоки относно операциите по обработване, за които „*съществува вероятност да породят висок риск*“, вж. бележка под линия 10 по-горе.

3.1.2 СЛУЧАЙ № 05 — Смекчаване на последиците и задължения

54. Ако това е възможно, след решаването на проблема базата данни следва да бъде сравнена с тази, която се съхранява в сигурно резервно копие. Извлеченият опит, свързан с нарушението, следва да се използва при актуализирането на ИТ инфраструктурата. Администраторът на лични данни следва да възстанови всички засегнати ИТ системи до познато чисто състояние, да отстрани уязвимостта и да въведе нови мерки за сигурност, за да се предотвратят подобни нарушения на сигурността на личните данни в бъдеще, т.е. проверки за целостта на файловете и проверки на сигурността. В случай че личните данни са не само изнесени, но и изтрити, администраторът трябва да предприеме системни действия, за да възстанови личните данни в състоянието, в което са били преди нарушението. Може да се наложи да се направят пълни резервни копия, поетапни промени и след това евентуално повторно изпълнение на обработката след последното поетапно архивиране, за което е необходимо администраторът да може да възпроизведе промените, направени след последното архивиране. Може да се наложи администраторът да проектира системата така, че ежедневните входящи файлове да се запазват, в случай че трябва да бъдат обработени отново, като е необходим надежден метод на съхранение и подходяща политика за запазване.

55. С оглед на гореизложеното, предвид факта, че има вероятност нарушението да породи висок риск за правата и свободите на физическите лица, субектите на данни определено следва да бъдат уведомени за него (член 34, параграф 1), което, разбира се, означава, че и съответният(те) НО следва да бъде(ат) запознат(и) с изпращане на уведомление за нарушение на сигурността на личните данни. Документирането на нарушението е задължително съгласно член 33, параграф 5 от ОРЗД и улеснява оценяването на ситуацията.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	✓

3.2 СЛУЧАЙ № 06: Ексфилтрация на хеширана парола от уебсайт

Уязвимост на SQL инжектиране е използвана за получаване на достъп до база данни на сървъра на готварски уебсайт. Потребителите са имали възможност да избират само произволни псевдоними като потребителско име. Препоръчвало се е да се избягва използването на адреси на електронна поща за тази цел. Пароли, съхранявани в базата данни, са били хеширани със силен алгоритъм и допълнението за удостоверяване към паролата не е било компрометирано. Засегнати данни: хеширани пароли на 1200 потребители. За целите на безопасността администраторът е уведомил субектите на данни за нарушението по електронна поща и ги е помолил да сменят своите пароли, особено ако същата парола е била използвана за други услуги.

3.2.1 СЛУЧАЙ № 06 — Предварителни мерки и оценка на риска

56. В този конкретен случай поверителността на данните е компрометирана, но паролите в базата данни са били хеширани с помощта на съвременен метод, което би намалило риска по отношение на естеството, чувствителността и обема на личните данни. Този случай не поражда рискове за правата и свободите на субектите на данни.

57. Освен това не е компрометирана и информацията за връзка (например адреси на електронна поща или телефонни номера) на субектите на данни, което означава, че няма сериозен риск субектите на данни да се превърнат в мишена на опити за измама (например получаване на фишинг имейли или на текстови съобщения и телефонни обаждания с цел измама). Не са замесени специални категории лични данни.

58. Някои потребителски имена можеха да се разглеждат като лични данни, но темата на уебсайта не позволява негативни асоциации. Трябва да се отбележи обаче, че оценката на риска може да се промени[20], ако видът на уебсайта и данните, до които е осъществен достъп, биха моли да разкрият специални категории лични данни (например уебсайт на политическа партия или синдикална организация). Използването на съвременно криптиране може да смекчи неблагоприятните последици от нарушението. Разрешаването на ограничен брой опити за влизане ще предотврати успешното реализиране на атаки на паролата с груба сила, по този начин намалявайки до голяма степен рисковете, породени от атакуващите, които вече знаят потребителските имена.

3.2.2 СЛУЧАЙ № 06 — Смекчаване на последиците и задължения

59. Уведомяването на субектите на данни в някои случаи би могло да се разглежда като смекчаващ фактор, тъй като субектите на данни са в състояние да предприемат необходимите стъпки за предотвратяване на по-нататъшни вреди от нарушението, например чрез смяна на своите пароли. В този случай уведомяването не е било задължително, но в много случаи може да се счита за добра практика.

60. Администраторът на лични данни следва да отстрани уязвимостта и да въведе нови мерки за сигурност, за да се предотвратят подобни нарушения на сигурността на личните данни в бъдеще, например систематични проверки на сигурността на уебсайта.

61. Нарушението следва да бъде документирано в съответствие с член 33, параграф 5, но не е необходимо да се изпраща уведомление или съобщение.

62. Също така силно се препоръчва на субектите на данни във всички случаи да се изпращат уведомления за нарушенията, свързани с пароли, дори когато паролите са съхранявани с помощта на хеш с допълнение за удостоверяване към паролата с алгоритъм, който отговаря на съвременното технологично равнище. Препоръчва се използването на методи за удостоверяване, които премахват необходимостта от обработка на паролите на сървъра. Субектите на данни следва да имат избор да предприемат подходящи мерки по отношение на собствените си пароли.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	X	X

[20] За насоки относно операциите по обработване, за които *„съществува вероятност да породят висок риск“*, вж. бележка под линия 10 по-горе.

3.3 СЛУЧАЙ № 07: Атака с пълнене на идентификационни данни на банков уебсайт

Банка претърпява кибератака срещу един от нейните уебсайтове за електронно банкиране. Атаката е имала за цел да изброи всички възможни идентификатори за вход на потребители, използващи лесна за разбиване фиксирана парола. Паролите съдържат 8 цифри. Поради уязвимостта на уебсайта в някои случаи информация относно субектите на данни (име, фамилия, пол, дата и място на раждане, данъчен код, кодове за идентификация на потребители) е изтекла към атакуващия, дори ако използваната парола не е била правилна или ако банковата сметка вече не е била активна. Това е засегнало около 100 000 субекти на данни. Атакуващият е успял да влезе в около 2 000 от тези профили, които са използвали лесната за разбиване парола, изпробвана от атакуващия. След атаката администраторът е успял да идентифицира всички опити за незаконно влизане. Администраторът на данни е успял да потвърди, след направени проверки за измама, че по време на атаката от тези профили не са извършени никакви трансакции. Банката е била запозната с нарушението на сигурността на личните данни, тъй като нейният център за операции по сигурността е засякъл висок брой заявки за вход, насочени към уебсайта. В отговор на това администраторът е дезактивирал възможността за влизане в уебсайта, като я е изключил и е приложил принудително нулиране на паролите на компрометираните профили. Администраторът е съобщил за нарушението само на потребителите с компрометирани профили, т.е. на потребителите, чиито пароли са били компрометирани или чиито данни са били разкрити.

3.3.1 СЛУЧАЙ № 07 — Предварителни мерки и оценка на риска

63. Важно е да се спомене, че администраторите, обработващи данни от изключително личен характер[21], имат по-голяма отговорност от гледна точка на осигуряването на адекватна сигурност на данните, например да разполагат с център за операции по сигурността и да са въвели други мерки за предотвратяване, откриване и реакция при инциденти. Неспазването на тези по-високи стандарти със сигурност ще доведе до по-сериозни мерки по време на разследване от страна на НО.

64. Нарушението засяга финансова информация, различна от информацията за самоличността и потребителското име, което го прави изключително сериозно. Броят на засегнатите физически лица е висок.

65. Фактът, че би могло да се случи нарушение в такава чувствителна среда, показва наличието на сериозни пропуски в сигурността на данните в системата на администратора и може да е показател, че е настъпил момент, в който преразглеждането и актуализирането на засегнатите мерки е „необходимо“ в съответствие с член 24, параграф 1, член 25, параграф 1 и член 32, параграф 1 от ОРЗД. Данните, попадащи в обхвата на нарушението, дават възможност за конкретно идентифициране на субектите на данни и съдържат друга информация за тях (включително пол, дата и място на раждане), а освен това могат да бъдат използвани от атакуващия за налучкване на паролите на клиентите или за провеждане на фишинг кампания, насочена към клиентите на банката.

[21] Като информация на субектите на данни, отнасяща се до начини на плащане, като номера на карти, банкови сметки, онлайн плащане, фишове за заплати, банкови извлечения, икономически проучвания, или всяка друга информация, която би могла да разкрие икономическа информация, свързана със субектите на данни.

66. Поради тази причина е счетено, че има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на всички засегнати субекти на данни[22]. Ето защо е възможно да настъпят имуществени (например финансова загуба) и неимуществени вреди (например кражба на самоличност или измама).

3.3.2 СЛУЧАЙ № 07 — Смекчаване на последиците и задължения

67. Мерките на администратора, споменати в описанието на случая, са адекватни. В резултат на нарушението той също така коригира уязвимостта на уебсайта и предприе други стъпки за предотвратяване на подобни нарушения на сигурността на личните данни в бъдеще, като добавяне на двуфакторно удостоверяване на засегнатия уебсайт и преминаване към задълбочено установяване на идентичността на клиента.

68. Документирането на нарушението в съответствие с член 33, параграф 5 от ОРЗД и уведомяването на НО за нарушението не са въпрос на избор в тази ситуация. Освен това администраторът следва да уведоми всички 100 000 субекти на данни (включително субектите на данни, чиито профили не са били компрометирани) в съответствие с член 34от ОРЗД.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	✓

3.4 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от хакерски атаки

69. Също като в случая с атаките със софтуер за изнудване, независимо от изхода и последиците от атаката, преразглеждането на сигурността на ИТ е задължително за администраторите в подобни случаи.

70. Препоръчителни мерки:[23]

(Списъкът със следващите мерки в никакъв случай не е изключителен или изчерпателен. Целта е да се предложат идеи за превенция и възможни решения. Всяка дейност по обработване е различна, поради което администраторът следва да вземе решение кои мерки най-добре пасват на дадената ситуация.)

- Съвременно криптиране и управление на ключове, особено когато се обработват пароли, чувствителни или финансови данни. Криптографското хеширане и добавяне на допълнения за удостоверяване към паролите по отношение на поверителната информация (пароли) винаги е за предпочитане пред криптирането на пароли. За предпочитане е използването на методи за удостоверяване, които премахват необходимостта от обработка на паролите на сървъра.
- Редовно актуализиране на системата (софтуер и софтуер на производителя). Въвеждане на всички мерки за сигурност на ИТ, гарантиране, че те са ефективни, и редовното им актуализиране, когато се променя или развива обработването или обстоятелствата. За да може да докаже съответствие с член 5,

[22] За насоки относно операциите по обработване, за които „*съществува вероятност да породят висок риск*“, вж. бележка под линия 10 по-горе.

[23] За сигурно разработване на уеб приложения, вж. също: https://www.owasp.org/index.php/Main_Page .

параграф 1, буква е) в съответствие с член 5, параграф 2 от ОРЗД, администраторът следва да поддържа регистър на всички направени актуализации, включително на момента, когато са изпълнени.

- Използване на силни методи за удостоверяване на автентичността като двуфакторно удостоверяване и сървъри за удостоверяване, допълнени от актуална политика относно паролите.
- Сигурните стандарти за разработка включват филтрирането на информацията, въведена от потребителите (с помощта на „бели“ списъци, доколкото е практически възможно), избягване на информацията, въведена от потребителите, мерки за предотвратяване на атаки с груба сила (като ограничаване на максималния брой повторни опити). „Защитните стени на уеб приложенията“ могат да помогнат за ефективното използване на тази техника.
- Има въведени силни права на потребителите и политика за управление на контрол на достъпа.
- Използване на подходяща, актуална, ефективна и интегрирана защитна стена, на система за установяване на проникване и на други системи за защита на периметъра.
- Системни проверки на сигурността на ИТ и оценки на уязвимостта (изпитване за пробив).
- Провеждане на редовни прегледи и изпитвания, за да се гарантира, че резервните копия могат да се използват за възстановяване на данните, чиято цялост или наличност са засегнати.
- Да не се поставя в обикновен текст идентификаторът на сесията в URL.

4 ВЪТРЕШЕН ИЗТОЧНИК НА РИСК, ПОРОДЕН ОТ РОЛЯТА НА ЧОВЕКА

71. Трябва да се обърне внимание на ролята на човешката грешка в нарушенията на сигурността на личните данни, тъй като тя е често срещана. Тези видове нарушения могат да бъдат както умишлени, така и неволни, ето защо е много трудно за администраторите на лични данни да идентифицират уязвимостите и да въведат мерки за тяхното предотвратяване. Международната конференция на комисарите по защита на личните данни и неприкосновеността на личния живот призна важността на справянето с тези човешки фактори и през октомври 2019 г. прие решение за справяне с ролята на човешката грешка в нарушенията на сигурността на личните данни[24]. В решението се подчертава, че подходящи защитни мерки следва да бъдат предприети за предотвратяване на човешки грешки, като е предвиден и неизчерпателен списък на такива мерки и подходи.

4.1 СЛУЧАЙ № 08: Ексфилтрация на бизнес данни от служител

По време на срока на своето предизвестие служител на дружество копира бизнес данни от базата данни на дружеството. Служителят има право да осъществява достъп до данните, само за да изпълнява служебните си задачи. Няколко месеца по-късно, след като служителят вече е напуснал работата, той използва данните, които е получил по този начин (базови данни за връзка), за нова обработка на данни, на която той е администратор, за да се свърже с клиентите на дружеството и да ги привлече към своя нов бизнес.

4.1.1 СЛУЧАЙ № 08 — Предварителни мерки и оценка на риска

72. В този конкретен случай не са били въведени предварителни мерки, с помощта на които да се предотврати копирането на информацията за връзка на клиентите на дружеството от служителя, тъй като той се е нуждаел и е имал разрешен достъп до тази информация, за да изпълнява своите служебни задачи. Тъй като за изпълнението на повечето задачи, свързани с връзката с клиенти, е необходим някакъв вид достъп

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

до лични данни от страна на служителите, може да се окаже, че тези нарушения на сигурността на личните данни е най-трудно да бъдат предотвратени. Ограниченията на обхвата на достъпа могат да ограничат работата, която даден служител може да изпълнява. Въпреки това добре обмислените политики за достъпа и постоянният контрол могат да помогнат за предотвратяване на този вид нарушения.

73. Както обикновено по време на оценката на риска трябва да се вземат под внимание видът на нарушението и естеството, чувствителността и обемът на засегнатите лични данни. Тези видове нарушения обикновено са нарушения на поверителността, тъй като базата данни по принцип се оставя непроменена, нейното съдържание „просто“ се копира за по-нататъшна употреба. Количеството засегнати данни обикновено е малко или средно. В този конкретен случай не са засегнати специални категории лични данни, служителят е имал нужда само от информацията за връзка с клиентите, за да може да се свърже с тях след като напусне дружеството. Ето защо засегнатите данни не са чувствителни.

74. Макар че единствената цел на бившия служител, който злонамерено е копирал данните, може да е само да получи информация за връзка с клиентите на дружеството за собствени търговски цели, администраторът не е в позиция да смята, че рискът за засегнатите субекти на данни е нисък, тъй като администраторът не може да бъде сигурен какви са намеренията на служителя. Ето защо, въпреки че последиците от нарушението могат да бъдат ограничени до излагането на нежелано самостоятелно предлагане от бившия служител, не може да се изключи вероятността за по-нататъшна и по-сериозна злоупотреба с откраднатите данни, в зависимост от целта на обработването, извършвано от него[25].

4.1.2 СЛУЧАЙ № 08 — Смекчаване на последиците и задължения

75. Смекчаването на неблагоприятните последици от нарушението, описано в горния случай, не е лесно. Може да се наложи предприемането на незабавни съдебни действия, за да се предотврати по-нататъшната злоупотреба и разпространение на личните данни от страна на бившия служител. Като следваща стъпка следва да се постави за цел избягването на подобни ситуации в бъдеще. Администраторът може да се опита да разпореди на бившия служител да спре да използва личните данни, но е малко вероятно това действие да има успешен край. Подходящи технически мерки като невъзможност за копиране или изтегляне на данни на подвижни устройства за съхранение биха могли да помогнат.

76. За тези случаи не съществува еднотипно решение, но наличието на системен подход може да помогне те да бъдат избегнати. Например в дружеството може да се помисли, когато това е възможно, дали да не бъдат оттеглени някои форми на достъп за служителите, които са уведомили, че желаят да напуснат, или да се въведат записи за достъп, така че по отношение на нежелания достъп да има запис и да е подаден сигнал. В договора, подписван със служителите, следва да се включват клаузи, забраняващи такива действия.

77. Като цяло, тъй като даденото нарушение няма да породи висок риск за правата и свободите на физическите лица, ще бъде достатъчно да се изпрати уведомление до НО. Информирането на субектите на данни може да е от полза и за администратора на лични данни, тъй като може би е по-добре да чуят за изтичането на данни от дружеството, а не от бившия служител, който прави опити да се свърже с тях. Документирането на нарушението на сигурността на личните данни е правно задължение в съответствие с член 33, параграф 5.

[25] За насоки относно операциите по обработване, за които „*съществува вероятност да породят висок риск*“, вж. бележка под линия 10 по-горе.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	X

4.2 СЛУЧАЙ № 09: Случайно предаване на данни към доверена трета страна

Застрахователен агент забелязва, че поради неправилните настройки на файл в Excel, получен по електронна поща, той може да осъществява достъп до информация, свързана с две дузини клиенти, които не са част от неговите клиенти. Той е задължен да пази служебна тайна и е бил единственият получател на електронната поща. Съгласно споразумението между администратора на лични данни и застрахователния агент, агентът е задължен незабавно да подаде сигнал към администратора на лични данни в случай на нарушение на сигурността на личните данни. Поради това агентът незабавно е подал сигнал за грешката на администратора на лични данни, който коригирал файла и отново го изпратил, като помолил агента да изтрие предишното съобщение. Съгласно гореспоменатото споразумение агентът трябва да потвърди изтриването в писмен вид, което и направил. В получената информация няма специални категории лични данни, а единствено данни за връзка и данни за самата застраховка (вид на застраховката, сума). След анализ на личните данни, засегнати от нарушението, администраторът на лични данни не е установил някакви специални характеристики от страна на физическите лица или на администратора на лични данни, които биха могли да засегнат нивото на въздействие от нарушението.

4.2.1 СЛУЧАЙ № 09 — Предварителни мерки и оценка на риска

78. Тук нарушението не е в резултат на умишлено действие на служител, а на неволна човешка грешка, причинена от невнимание. Тези видове нарушения могат да бъдат избегнати или намалени по честота посредством а) задължително въвеждане на програми за обучение, образование и повишаване на осведомеността, с помощта на които служителите научават повече за значението на защитата на личните данни, б) намаляване на изпращането на файлове по електронна поща, вместо това могат да се използват специални системи за обработване на клиентски данни например, в) извършване на двойна проверка на файловете преди изпращане, г) разделяне на операциите по създаване и изпращане на файлове.

79. Това нарушение на сигурността на личните данни засяга единствено поверителността на данните, докато тяхната цялост и достъпност са останали непокътнати. Нарушението на сигурността на личните данни е засегнало само около две дузини клиенти, поради което количеството на засегнатите данни може да се разглежда като ниско. Освен това засегнатите лични данни не са съдържали никакви чувствителни данни. Фактът, че обработващият лични данни без забавяне се е свързал с администратора на лични данни, след като е разбрал за нарушението на сигурността на личните данни, може да се разглежда като фактор, който намалява риска. (Следва да се оцени и възможността данните да са били изпратени на други застрахователни агенти и ако това се потвърди, следва да бъдат взети подходящи мерки.) Тъй като след нарушението на сигурността на личните данни са предприети подходящи стъпки, то вероятно няма да има въздействие върху правата и свободите на субектите на данни.

80. Поради комбинацията от малкия брой засегнати физически лица, незабавното засичане на нарушението и мерките, предприети за смекчаване на неговите последици, този конкретен случай не поражда риск.

4.2.2 СЛУЧАЙ № 09 — Смекчаване на последиците и задължения

81. Освен това и други смекчаващи обстоятелства оказват влияние: агентът е задължен да пази служебна тайна; той самият е съобщил за проблема на администратора; и при поискване е изтрил файла. Има вероятност повишаването на информираността и евентуалното включване на допълнителни стъпки при проверката на документи, включващи лични данни, да помогне за предотвратяването на подобни случаи в бъдеще.

82. Освен документирането на нарушението в съответствие с член 33, параграф 5, не са необходими други действия.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	X	X

4.3 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от вътрешните източници на риск, породен от ролята на човека

83. Комбинация от мерките, посочени по-долу, приложени в зависимост от конкретните характеристики на случая, следва да помогне за намаляване на възможността за повторна поява на подобно нарушение.

84. Препоръчителни мерки:

(Списъкът със следващите мерки в никакъв случай не е изключителен или изчерпателен. Целта е да се предложат идеи за превенция и възможни решения. Всяка дейност по обработване е различна, поради което администраторът следва да вземе решение кои мерки най-добре пасват на дадената ситуация.)

- Периодично изпълнение на програми за обучение, образование и повишаване на осведомеността на служителите относно техните задължения, свързани с опазването на поверителността и сигурността, и засичането, и изпращането на сигнали за заплахи за сигурността на лични данни[26]. Създаване на програма за осведоменост, която да припомня на служителите кои са най-често срещаните грешки, водещи до нарушения на сигурността на личните данни, и как да бъдат избегнати.
- Разработване на надеждни и ефективни практики, процедури и системи за защита на данните и неприкосновеността на личния живот[27].
- Оценка на практиките, процедурите и системите за поверителност, за да се гарантира непрекъсната ефективност[28].
- Разработване на подходящи политики за контрол на достъпа и въвеждане на задължение за потребителите да спазват правилата.
- Въвеждане на техники за задължително удостоверяване на самоличността на потребителя при осъществяване на достъп до чувствителни лични данни.
- Дезактивиране на профила на потребителя в дружеството веднага щом лицето напусне дружеството.
- Извършване на проверка на необичайни потоци от данни между файловия сървър и работните станции на служителите.
- Разработване на сигурен входно-изходен интерфейс в BIOS или с помощта на софтуер, който контролира използването на компютърен интерфейс (заключване или отключване, например USB/CD/DVD и т.н.).
- Преглед на политиката за достъп на служителите (например регистриране на достъпа до чувствителни данни и поставяне на изискване към потребителя да вписва служебна причина, така че тази информация да бъде на разположение при проверки).

[26] Раздел 2), подраздел i) от Решението за справяне с ролята на човешката грешка в нарушенията на сигурността на личните данни.

[27] Раздел 2), подраздел ii) от Решението за справяне с ролята на човешката грешка в нарушенията на сигурността на личните данни.

[28] Раздел 2), подраздел iii) от Решението за справяне с ролята на човешката грешка в нарушенията на сигурността на личните данни.

- Дезактивиране на облачните услуги с отворен код.
- Забраняване и предотвратяване на достъпа до известни пощенски услуги с отворен код.
- Дезактивиране на функцията за снимка на екрана в OS.
- Налагане на политика на „чистото бюро“.
- Автоматично заключване на всички компютри след определен период на неактивност.
- Използване на механизми (например (безжично) токен устройство за идентификация/отваряне на заключени профили) за бърза смяна на потребители в споделени среди.
- Използване на специални системи за управление на личните данни, които прилагат подходящи механизми за контрол на достъпа и които предотвратяват човешката грешка, като изпращане на съобщения на грешен субект. Използването на електронни таблици и други офис документи не е подходящ начин за управление на данни на клиентите.

5 ИЗГУБЕНИ ИЛИ ОТКРАДНАТИ УСТРОЙСТВА И ДОКУМЕНТИ НА ХАРТИЯ

85. Често срещан случай е загубата или кражбата на преносими устройства. В тези случаи, за да гарантира подходящо ниво на сигурност, администраторът трябва да вземе под внимание обстоятелствата на операцията по обработване, като вида на данните, съхранявани на устройството, както и спомагателните активи, и предприетите мерки преди нарушението.. Всички тези елементи оказват влияние върху потенциалното въздействие на нарушението на сигурността на личните данни. Възможно е оценката на риска да е трудна, тъй като устройството вече не е налично.

86. Тези видове нарушения винаги могат да бъдат класифицирани като нарушения на поверителността. В случай че няма резервно копие на откраднатата база данни, обаче, нарушението може да се определи и като нарушение на наличността и нарушение на целостта.

87. Сценариите, описани по-долу, показват как гореспоменатите обстоятелствата оказват влияние върху вероятността и сериозността на нарушението на сигурността на личните данни.

5.1 СЛУЧАЙ № 10: Откраднат материал, в който са се съхранявали криптирани лични данни

При влизане с взлом в център за дневни детски грижи са откраднати два таблетни компютъра. Таблетните компютри съдържали приложение, в което се съхранявали лични данни за децата, посещаващи дневния център. Засегнати са име, дата на раждане, лични данни за обучението на децата. Както криптираните таблетни компютри, които в момента на влизането с взлом са били изключени, така и приложението са били защитени с надеждна парола. Администраторът е разполагал с леснодостъпно резервно копие на данните. Скоро след откриването на влизането с взлом, дневният център издава команда за изтриване на информацията в таблетните компютри от разстояние.

5.1.1 СЛУЧАЙ № 10 — Предварителни мерки и оценка на риска

88. В конкретния случай администраторът на лични данни е предприел адекватни мерки, за да избегне и смекчи въздействието на евентуално нарушение на сигурността на личните данни, като е използвал криптиране на устройството, въвел е адекватна защита с парола и е осигурил резервно копие на данните, съхранявани на таблетните компютри. (Списък с препоръчителни мерки може да бъде намерен в раздел 5.7).

89. След като разбере за нарушението, администраторът на лични данни следва да определи източника на риска, системите, поддържащи обработването на лични данни, видът на засегнатите лични данни и потенциалното въздействие на нарушението на сигурността върху засегнатите физически лица. Гореописаното нарушение на сигурността на личните данни би могло да засегне поверителността, наличността и целостта на данните, но поради адекватните действия на администратора преди нарушението на сигурността на личните данни и след това, нито едно от горните неща не се е случило.

5.1.2 СЛУЧАЙ № 10 — Смекчаване на последиците и задължения

90. Поверителността на личните данни, намиращи се на устройствата, не е компрометирана поради надеждната защита с парола, както на двата таблетни компютъра, така и на приложенията. Таблетните компютри са били настроени по такъв начин, че задаването на парола е означавало също, че данните, намиращи се на устройството, се криптират. Това е допълнително подпомогнато от действията на администратора за изтриване от разстояние на всичко от откраднатите устройства.

91. Поради предприетите мерки поверителността на данните е останала непокътната. Освен това резервното копие е осигурило непрекъсната наличност на личните данни, следователно не е имало вероятност да възникне потенциално отрицателно въздействие.

92. Поради тези факти не е имало вероятност описаното по-горе нарушение на сигурността на личните данни да породи риск за правата и свободите на субектите на данни, следователно не е било необходимо да се изпраща уведомление до НО или до засегнатите субекти на данни. Това нарушение на сигурността на личните данни обаче трябва да бъде документирано в съответствие с член 33, параграф 5.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	X	X

5.2 СЛУЧАЙ № 11: Откраднат материал, в който са се съхранявали некриптирани лични данни

Откраднат е лаптопът на служител на дружество, предоставящо услуги. В откраднатия лаптоп са се съхранявали имената, фамилиите, пола, адресите и датите на раждане на повече от 100 000 клиента. Поради факта, че откраднатото устройство не е налично, няма възможност да се установи дали са засегнати и други категории лични данни. Достъпът до твърдия диск на лаптопа не е защитен с парола. Личните данни е възможно да бъдат възстановени от наличните ежедневни резервни копия.

5.2.1 СЛУЧАЙ № 11 — Предварителни мерки и оценка на риска

93. Администраторът на лични данни не е предприел никакви предварителни мерки за сигурност, поради което личните данни, съхранявани в откраднатия лаптоп, са били лесно достъпни за крадеца или за всяко друго лице, което разполага с устройството след това.

94. Това нарушение на сигурността на личните данни засяга поверителността на данните, съхранявани на откраднатото устройство.

95. Лаптопът, съхраняващ личните данни, в този случай е бил уязвим, защото не е имал защита с парола или криптиране. Липсата на основни мерки за сигурност повишава нивото на риска за засегнатите субекти на данни. Освен това идентифицирането на засегнатите субекти на данни също представлява проблем, което допълнително увеличава сериозността на нарушението. Големият брой засегнати физически лица увеличава риска, но при нарушението на сигурността не са засегнати специални категории лични данни.

96. По време на оценката на риска[29] администраторът следва да вземе под внимание потенциалните последици и неблагоприятни въздействия на нарушението на поверителността. В резултат на нарушението засегнатите субекти на данни биха могли да станат жертва на измама с използване на фалшива самоличност поради наличието на данни на откраднатото устройство, така че рискът се счита за висок.

5.2.2 СЛУЧАЙ № 11 — Смекчаване на последиците и задължения

97. Включването на криптиране на устройството и използването на надеждна парола за защита на съхраняваната база данни е можело да предотврати възможността нарушението на сигурността на личните данни да породи риск за правата и свободите на субектите на данни.

98. Поради тези обстоятелства уведомяването на НО е наложително, но също така е необходимо да бъдат уведомени и засегнатите субекти на данни.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	✓

5.3 СЛУЧАЙ № 12: Откраднати досиета на хартиен носител с чувствителни данни

Дневник на хартиен носител е откраднат от център за рехабилитация на зависими от наркотици. В дневника са се съдържали основни данни за самоличност и здравни данни на пациентите, приети в центъра за рехабилитация. Данните са се съхранявали само на хартиен носител и лекарите, лекуващи пациентите, не са разполагали с резервно копие. Дневникът не се е съхранявал в заключено чекмедже или стая, администраторът на лични данни не е бил въвел нито режим за контрол на достъпа, нито други предпазни мерки за документацията на хартиен носител.

5.3.1 СЛУЧАЙ № 12 — Предварителни мерки и оценка на риска

99. Администраторът на лични данни не е предприел никакви предварителни мерки за сигурност, поради което личните данни, съхранявани в този дневник, са били лесно достъпни за лицето, което го е намерило. Освен това естеството на личните данни, съхранявани в дневника, превръща липсата на резервни данни в много сериозен рисков фактор.

100. Този случай служи като пример за нарушение на сигурността на личните данни, пораждащо висок риск. Поради неспазване на изискването за въвеждане на подходящи мерки за сигурност, са загубени чувствителни данни за здравословното състояние съгласно член 9, параграф 1 от ОРЗД. Тъй като в този случай е засегната специална категория лични данни, потенциалните рискове за засегнатите субекти на данни са по-високи, което следва да бъде взето под внимание при оценката на риска от страна на администратора на данни[30].

101. Това нарушение е свързано с поверителността, наличието и целостта на засегнатите лични данни. В резултат на нарушението е нарушена медицинската тайна и неоправомощени трети лица биха могли да получат достъп до личната медицинска информация на пациентите, което може да има сериозно

[29] За насоки относно операциите по обработване, за които *„съществува вероятност да породят висок риск“*, вж. бележка под линия 10 по-горе.

[30] За насоки относно операциите по обработване, за които *„съществува вероятност да породят висок риск“*, вж. бележка под линия 10 по-горе.

въздействие върху личния живот на пациента. Нарушението на наличността може също така да повлияе на непрекъснатостта на лечението на пациентите. Тъй като не може да се изключи вероятността части от съдържанието на дневника да бъдат променени/изтрити, целостта на личните данни също е компрометирана.

5.3.2 СЛУЧАЙ № 12 — Смекчаване на последиците и задължения

102. При оценката на защитните мерки следва да се вземе предвид и видът на спомагателния актив. Тъй като пациентският дневник е физически документ, неговото опазване е следвало да бъде организирано по различен начин от този за електронно устройство. Псевдонимизацията на имената на пациентите, съхранението на дневника в защитени помещения и в заключено чекмедже или стая, както и подходящият контрол с удостоверяване на автентичността при достъп са можели да предотвратят нарушението на сигурността на личните данни.

103. Има вероятност нарушението на сигурността на личните данни, описано по-горе, да доведе до сериозни последици за засегнатите субекти на данни; поради това уведомяването на НО и съобщаването за нарушението на засегнатите субекти на данни е задължително.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	ащане на съобщение до субектите на данни
✓	✓	✓

5.4 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от загубата или кражбата на устройства

104. Комбинация от мерките, посочени по-долу, приложени в зависимост от конкретните характеристики на случая, следва да помогне за намаляване на възможността за повторна поява на подобно нарушение.

105. Препоръчителни мерки:

(*Списъкът със следващите мерки в никакъв случай не е изключителен или изчерпателен. Целта е да се предложат идеи за превенция и възможни решения. Всяка дейност по обработване е различна, поради което администраторът следва да вземе решение кои мерки най-добре пасват на дадената ситуация.)*

- Включване на криптирането на устройството (като Bitlocker, Veracrypt или DM-Crypt).
- Използване на код за достъп/парола на всички устройства. Криптиране на всички мобилни електронни устройства по начин, който изисква въвеждането на сложна парола за декриптиране.
- Използване на многофакторно удостоверяване.
- По отношение на устройства с висока мобилност — включване на функциите, които създават възможност местоположението им да бъде открито в случай на загуба или поставяне на неправилно място.
- Използване на софтуер/приложение за управление на преносими устройства (MDM) и определяне на местоположението. Използване на филтри срещу отблясъци. Затваряне на устройствата без надзор.
- Ако е възможно и подходящо за обработването на лични данни, което се разглежда, запазване на личните данни не на преносимо устройство, а на централен вътрешен сървър.
- В случай че работната станция е свързана към корпоративната локална мрежа, извършване на автоматично архивиране от работните папки, при условие че е неизбежно личните данни да се съхраняват там.
- Използване на сигурна локална мрежа (например която изисква отделен втори ключ за факторно удостоверяване за създаване на защитена връзка) за свързване на мобилни устройства към вътрешни сървъри.

- Осигуряване на заключващи устройства на служителите, за да имат възможност физически да защитят използваните от тях преносими устройства, когато ги оставят без надзор.
- Необходимост от правилно регулиране на използването на устройствата извън дружеството.
- Необходимост от правилно регулиране на използването на устройствата в рамките на дружеството.
- Използване на софтуер/приложение за управление на преносими устройства (MDM) и активиране на функцията за изтриване от разстояние.
- Използване на централизирано управление на устройствата със сведени до минимум права за инсталиране на софтуер на крайните потребители.
- Инсталиране на физически механизми за контрол на достъпа.
- Избягване на съхраняването на чувствителна информация на преносими устройства или твърди дискове. В случай че е необходимо да се осъществява достъп до вътрешната система на дружеството, следва да се използват сигурни канали, като описаните по-горе.

6 ПОГРЕШНО ИЗПРАЩАНЕ НА ПОЩЕНСКА ПРАТКА

106. И в този случай източникът на риска е вътрешна човешка грешка, но тук причината за нарушението не е злонамерено действие. То е в резултат на невнимание. След възникването на грешката администраторът може да направи само ограничен брой неща, поради което предотвратяването в тези случаи е дори по-важно, отколкото при други видове нарушения.

6.1 СЛУЧАЙ № 13: Грешка при изпращане на пощенска пратка

Две поръчки за обувки са опаковани от дружество за търговия на дребно. Поради човешка грешка двете товарителници са объркани, в резултат на което както продуктите, така и съответните товарителници са изпратени на грешния човек. Това означава, че всеки един от двамата клиенти получава поръчката на другия, включително и товарителниците, съдържащи личните данни. След като разбира за нарушението администраторът на лични данни успява да изземе поръчките и да ги изпрати на правилните получатели.

6.1.1 СЛУЧАЙ № 13 — Предварителни мерки и оценка на риска

107. Товарителниците са съдържали личните данни, необходими за успешното изпълнение на доставка (име, адрес, както и изделието и неговата цена). На първо място е важно да се установи как е могла да възникне човешката грешка и дали е имало начин да бъде предотвратена. В този конкретен случай рискът е нисък, тъй като не са засегнати специални категории лични данни или други данни, злоупотребата с които би могла да доведе до значителни отрицателни последици, нарушението не е възникнало в резултат на системна грешка от страна на администратора и само две физически лица са засегнати. Не са идентифицирани отрицателни последствия за физическите лица.

6.1.2 СЛУЧАЙ № 13 — Смекчаване на последиците и задължения

108. Администраторът следва да осигури безплатно връщане на изделията и придружаващите ги товарителници, както и да поиска от грешните получатели да унищожат/изтрият всички евентуални копия на товарителниците, съдържащи лични данни на другото лице.

109. Дори ако самото нарушение не поражда висок риск за правата и свободите на засегнатите лица и поради това съобщаването на субектите на данни не е задължително съгласно член 34 от ОРЗД, изпращането на съобщение до тях относно нарушението не може да бъде избегнато, тъй като е необходимо тяхното сътрудничество за смекчаване на риска.

Необходими действия въз основа на установените рискове

Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	X	X

6.2 СЛУЧАЙ № 14: Силно поверителни лични данни, изпратени по пощата по погрешка

Отделът по наемане на служители на публична администрация изпраща електронна поща относно предстоящи обучения на физическите лица, регистрирани в неговата система като лица, търсещи работа. По погрешка към тази електронна поща е прикачен документ, съдържащ личните данни на всички тези лица, търсещи работа (име, адрес на електронна поща, пощенски адрес, социалноосигурителен номер). Броят на засегнатите физически лица надхвърля 60 000. Впоследствие службата се свързва с всички получатели и ги моли да изтрият предишното съобщение и да не използват информацията, съдържаща се в него.

6.2.1 СЛУЧАЙ № 14 — Предварителни мерки и оценка на риска

110. За изпращането на такива съобщения е следвало да бъдат въведени по-строги правила. Трябва да се обмисли въвеждането на допълнителни механизми за контрол.

111. Броят на засегнатите физически лица е значителен, а това, че е замесен и техният социалноосигурителен номер, наред с други по-базови лични данни, допълнително повишава риска, който може да се определи като висок[31]. Администраторът не може да спре евентуалното разпространение на данните от някой от получателите.

6.2.2 СЛУЧАЙ № 14 — Смекчаване на последиците и задължения

112. Както беше споменато по-рано, средствата за ефективно смекчаване на рисковете от подобно нарушение са ограничени. Въпреки че администраторът е помолил съобщението да бъде изтрито, той не може да принуди получателите да го направят и в резултат на това не може да бъде сигурен, че те са се отзовали на молбата.

113. Изпълнението на всичките три действия, посочени по-долу, следва да е повече от ясно в случай като този.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	✓

6.3 СЛУЧАЙ № 15: Лични данни, изпратени по пощата по погрешка

Списък с участниците в курс по юридически английски език, който се провежда в хотел в продължение на 5 дни, по погрешка е изпратен на 15 бивши участници в курса, вместо до хотела. Списъкът съдържа имената, адресите на електронната поща и предпочитанията по отношение на храната на 15-те участника. Само двама от участниците са попълнили своите предпочитания по отношение на храната, като са обяснили, че имат непоносимост към лактозата. Нито един от участниците не е със защитена самоличност. Администраторът открива грешката веднага след изпращането на списъка и уведомява получателите за грешката, като ги моли да изтрият списъка.

[31] За насоки относно операциите по обработване, за които *„съществува вероятност да породят висок риск“*, вж. бележка под линия 10 по-горе.

6.3.1 СЛУЧАЙ № 15 — Предварителни мерки и оценка на риска

114. За изпращането на съобщения, съдържащи лични данни, е следвало да бъдат въведени по-строги правила. Трябва да се обмисли въвеждането на допълнителни механизми за контрол.

115. Рисковете, произтичащи от естеството, чувствителността, обема и контекста на личните данни, са малки. Личните данни включват чувствителни данни за предпочитанията по отношение на храната на двама от участниците. Дори и ако информацията, че някой има непоносимост към лактозата, представлява данни за здравословното състояние, рискът тези данни да бъдат използвани по начин, причиняващ вреда, следва да се счита за сравнително нисък. Въпреки че в случаите на данни за здравословното състояние обикновено се приема, че има вероятност нарушението да породи висок риск за субектите на данни[32], в този конкретен случай не може да се идентифицира риск нарушението до доведе до имуществени или неимуществени вреди за субекта на данни поради неразрешеното разкриване на информацията за непоносимост към лактозата. За разлика от някои други предпочитания по отношение на храната, непоносимостта към лактозата не може да бъде свързана с религиозни или философски убеждения. Също така са много малки количеството на данните, попадащи в обхвата на нарушението, и броят на засегнатите субекти на данни.

6.3.2 СЛУЧАЙ № 15 — Смекчаване на последиците и задължения

116. Накратко, може да се твърди, че нарушението не е имало сериозни последствия за субектите на данни. Фактът, че администраторът незабавно се е свързал с получателите, след като е узнал за грешката, може да се разглежда като смекчаващ фактор.

117. Ако електронна поща е изпратена до грешен/неупълномощен получател, се препоръчва администраторът на лични данни да изпрати последваща електронна поща до грешните получатели, използвайки функцията за скрито копие („Bcc“), в която се извинява и дава указания за изтриването на погрешно изпратената електронна поща, както и информира получателите, че те нямат право да използват адресите на електронна поща, които са им станали известни.

118. Поради тези факти не е имало вероятност това нарушение на сигурността на личните данни да породи риск за правата и свободите на субектите на данни, следователно не е било необходимо да се изпраща уведомление до НО или до засегнатите субекти на данни. Това нарушение на сигурността на личните данни обаче трябва да бъде документирано в съответствие с член 33, параграф 5.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	X	X

6.4 СЛУЧАЙ № 16: Грешка при изпращане на пощенска пратка

[32] Вж. Насоките на WP 250, стр. 23.

Застрахователна група предлага автомобилни застраховки. За тази цел тя изпраща периодично преизчислени полици по пощата. Освен името и адреса на титуляря на полицата писмото съдържа регистрационния номер на превозното средство, без скрити цифри, размера на застрахователните премии за настоящата и следващата застрахователна година, приблизителния годишен пробег и датата на раждане на титуляря на полицата. Не са включени данни за здравословното състояние съгласно член 9 от ОРЗД, данни за плащания (банкови данни), икономически и финансови данни.

Писмата се подготвят от автоматизирани машини за опаковане в плик. Поради механична грешка две писма за различни титуляри на полици са поставени в един плик и изпратени на един титуляр на полица по пощата. Титулярят на полицата отваря писмото вкъщи и поглежда своето правилно изпратено писмо, както и писмото, доставено по погрешка, за друг титуляр на полица.

6.4.1 СЛУЧАЙ № 16 — Предварителни мерки и оценка на риска

119. В изпратеното по погрешка писмо се съдържат името, адресът, датата на раждане, нескритият регистрационен номер на превозното средство и класификацията на размера на застрахователната премия за настоящата и следващата година. Сериозността на последиците за засегнатото лице трябва да се разглежда като умерена, тъй като информация, която не е обществено достъпна, като датата на раждане или нескритият регистрационен номер на превозното средство, както и подробности за нарастването на размера на застрахователната премия, са разкрити на неупълномощен получател. Вероятността за злоупотреба с тези данни се оценява на ниска или средна. И въпреки че много получатели вероятно ще изхвърлят грешното писмо в боклука, в отделни случаи не може напълно да бъде отхвърлена вероятността писмото да бъде публикувано в социалните мрежи или да се осъществи контакт с този титуляр на полица.

6.4.2 СЛУЧАЙ № 16 — Смекчаване на последиците и задължения

120. Администраторът следва да организира връщането на оригиналния документ за своя сметка. Грешният получател също така следва да бъде информиран, че той/тя няма право да злоупотребява с прочетената информация.

121. Вероятно никога няма да бъде възможно напълно да се предотвратят грешките в пощенските доставки при изпращане на голям брой пратки, при които се използват автоматизирани машини. В случай че честотата на грешките обаче се увеличи, е необходимо да се провери дали машините за опаковане в плик са настроени добре, и дали се поддържат правилно, или дали друг системен проблем не е причина за такова нарушение.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	X

6.5 Организационни и технически мерки за предотвратяване/смекчаване на въздействието от погрешно изпращане на пощенски пратки

122. Комбинация от мерките, посочени по-долу, приложени в зависимост от конкретните характеристики на случая, следва да помогне за намаляване на възможността за повторна поява на подобно нарушение.

123. Препоръчителни мерки:

(*Списъкът със следващите мерки в никакъв случай не е изключителен или изчерпателен. Целта е да се предложат идеи за превенция и възможни решения. Всяка дейност по обработване е различна,*

поради което администраторът следва да вземе решение кои мерки най-добре пасват на дадената ситуация.)

- Определяне на точни стандарти, без възможност за тълкуване, за изпращането на писма/електронна поща.
- Подходящо обучение на персонала за изпращането на писма/електронна поща.
- Когато се изпраща електронна поща до голям брой получатели, те по подразбиране трябва да бъдат изброявани в полето „bcc“ (скрито копие).
- Допълнително потвърждение е необходимо, когато се изпраща електронна поща до голям брой получатели и те не са изброени в полето „bcc“ (скрито копие).
- Прилагане на принципа на двойната проверка.
- Използване на автоматично вместо ръчно адресиране, при което данните се извличат от налична актуална база данни; на системата за автоматично адресиране следва да се прави редовен преглед, за да се проверява за скрити грешки и неправилни настройки.
- Използване на опция за забавяне на изпращането на съобщението (например- съобщението може да бъде изтрито/редактирано в рамките на определено време след щракване на бутона).
- Дезактивиране на функцията за автоматично довършване при въвеждане на адреси на електронна поща.
- Организиране на сесии за повишаване на информираността относно най-често срещаните грешки, които водят до нарушение на сигурността на личните данни.
- Обучения и наръчници по темата за справяне с инцидентите, които водят до нарушение на сигурността на личните данни, и на кого да се изпрати уведомление (с участието на длъжностното лице по защита на данните).

7 ДРУГИ СЛУЧАИ — СОЦИАЛНО ИНЖЕНЕРСТВО

7.1 СЛУЧАЙ № 17: Кражба на самоличност

Контактният център на телекомуникационно дружество получава телефонно обаждане от лице, което се представя за клиент. Предполагаемият клиент желае дружеството да промени адреса на електронната поща, на която следва да се изпраща информацията за сметката от този момент нататък. Служителят на контактния център потвърждава самоличността на клиента като задава въпроси, свързани с определени лични данни, както е определено в процедурите на дружеството. Лицето, което се обажда, правилно посочва изискания данъчен номер и пощенски адрес на клиента (тъй като е имал достъп до тези елементи). След потвърждаването операторът прави заявената промяна и от този момент нататък информацията за сметката се изпраща на новия адрес на електронна поща. В процедурата не е предвидено изпращане на уведомление до предишната електронна поща. През следващия месец истинският клиент се свързва с дружеството и желае да разбере защо не получава сметка на своята електронна поща, като отрича да се е обаждал с искане за промяна на електронната поща за връзка. На по-късен етап дружеството разбира, че информацията е изпратена на нелегитимен потребител и отменя промяната.

7.1.1 СЛУЧАЙ № 17 — Оценка на риска, смекчаване на последиците и задължения

124. Този случай служи като пример за значението на предварителните мерки. От гледна точка на риска нарушението поражда висок риск[33], тъй като в данните за фактуриране може да се съдържа информация за личния живот на субекта на данни (например навици, контакти) и това може да доведе до имуществена вреда (например преследване, риск за физическата неприкосновеност). Личните данни, получени по време на тази атака, могат също да се използват, за да се улесни „превземането“ на профила в тази организация или да се използват допълнителни мерки за удостоверяване на автентичността в други организации. Като се имат предвид тези рискове, „подходящата“ мярка за удостоверяване следва да отговаря на висок стандарт, в зависимост от това какви лични данни могат да бъдат обработвани в резултат на удостоверяването.

125. В резултат на това е необходимо администраторът да изпрати както уведомление до НО, така и съобщение до субекта на данни.

126. С оглед на този случай предишната процедура по потвърждаване на самоличността на клиента очевидно трябва да бъде усъвършенствана. Използваните методи за удостоверяване не са били достатъчни. Злонамерената страна е успяла да се престори на желания потребител с използване на обществено достъпна информация и информация, до която е имала достъп по друг начин.

127. Използването на този вид статичен метод на удостоверяване на база знания (където отговорът не се променя и информацията не е „тайна“, какъвто би бил случаят с парола) не се препоръчва.

128. Вместо това организацията следва да използва форма на удостоверяване, която би довела до висока степен на увереност, че потребителят, чиято самоличност е била удостоверена, е търсеното лице, а не някой друг. Въвеждането на различен от нормалното метод на многофакторно удостоверяване би решило този проблем, като например за да се потвърди дадена заявка за промяна, да е необходимо да се изпрати заявка за потвърждение на предишната точка за контакт; или добавяне на допълнителни въпроси и искане да се предостави информация, която може да се види само на предишни сметки. Отговорност на администратора е да реши какви мерки да въведе, тъй като той е най-добре запознат с особеностите и изискванията на вътрешната дейност.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	✓

7.2 СЛУЧАЙ № 18: Ексфилтрация по електронна поща

[33] За насоки относно операциите по обработване, за които „*съществува вероятност да породят висок риск*“, вж. бележка под линия 10 по-горе.

Верига от хипермаркети открива, 3 месеца след конфигурирането, че някои адреси на електронна поща са били променени и са създадени правила, според които всяка електронна поща, съдържаща определени изрази (като например „фактура“, „плащане“, „банков превод“, „потвърждаване на транзакции от кредитни карти“, „ данни за банкова сметка“), се премества в неизползвана папка и също така се препраща към външен адрес на електронна поща. Също така по това време вече е била реализирана атака, направена със средствата на социалното инженерство, т.е. атакуващият, представяйки се за доставчик, е бил подменил данните за банковата сметка на този доставчик със своите собствени данни. И накрая, по това време вече са били изпратени няколко фалшиви фактури, включващи новите данни за банкова сметка. В крайна сметка системата за наблюдение на платформата за електронна поща известява за папките. Като за начало, дружеството не успява да разкрие как атакуващият е успял да получи достъп до адресите на електронна поща, но предполага, че заразена електронна поща може да е причината за осигуряването на достъп до групата потребители, отговарящи за плащанията.

Тъй като препращането на електронна поща се извършва на базата на ключова дума, атакуващият е получил информация за 99 служители: име и заплата за определен месец за 89 субекти на данни; име, гражданско състояние, брой деца, заплата, работно време, както и остатъчна информация за получена заплата от 10 служители, чиито договори са прекратени. Администраторът уведомил само 10-те служители, които са част от последната група.

7.2.1 СЛУЧАЙ № 18 — Оценка на риска, смекчаване на последиците и задължения

129. Дори ако целта на атакуващия не е била събирането на лични данни, тъй като нарушението може да доведе както до имуществена (например- финансова загуба), така и до неимуществена вреда (например- кражба на самоличност или измама), или данните биха могли да се използват за улесняване на други атаки (например- фишинг), има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица. Ето защо съобщение за нарушението следва да се изпрати до всички 99 служители, а не само до 10-те служители, за чиито заплати е изтекла информация.

130. След като разбира за нарушението, администраторът разпорежда да се смени паролата за компрометираните профили, блокира изпращането на електронна поща до адреса на електронна поща на атакуващия, уведомява доставчика на услугата за електронна поща, използван от атакуващия, относно неговите действия, премахва правилата, зададени от атакуващия, и прецизира известията на системата за наблюдение, така че да се изпраща известие веднага щом бъде създадено автоматично правило. Друга възможност за администратора е да премахне правото на потребителите да задават правила за препращане и да изиска екипът за обслужване на ИТ системите да го прави само при поискване. Той също така може да въведе политика, съгласно която потребителите в отделите, обработващи финансови данни, следва да проверяват и докладват за правилата, зададени в техните профили, веднъж седмично или по-често.

131. Фактът, че един пробив може да се случи и да не бъде забелязан толкова дълго, и фактът, че за по-дълъг период от време социалното инженерство е можело да се използва за промяна на повече данни, показват, че в системата за сигурност на ИТ на администратора има сериозни проблеми. Незабавно следва да бъдат взети мерки за решаването им, като наблягане на прегледите на автоматизираната обработка и на контрола на промените, на откриването на инциденти и на мерките за реакция. Администраторите, обработващи чувствителни данни, финансова информация и т.н., имат по-голяма отговорност от гледна точка на осигуряването на адекватна сигурност на данните.

Необходими действия въз основа на установените рискове		
Вътрешно документиране	Уведомяване на НО	Изпращане на съобщение до субектите на данни
✓	✓	✓