Wytyczne 01/2021

w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

przyjęte 14 grudnia 2021 r.

wersja 2.0

Historia wersji

Wersja 2.0	14.12.2021 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	14.01.2021 r.	Przyjęcie wytycznych do konsultacji publicznych

Spis treści

EUROPEJSKA RADA OCHRONY DANYCH,

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i art. 22 swojego regulaminu wewnętrznego,

uwzględniając komunikat Komisji do Parlamentu Europejskiego i Rady pt. „Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych"[2],

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1 WPROWADZENIE

1. W RODO wprowadzono, w określonych przypadkach, wymóg zgłoszenia naruszenia ochrony danych osobowych właściwemu krajowemu organowi nadzorczemu (zwanemu dalej „organem nadzorczym") oraz zawiadomienia o naruszeniu osób, których dane osobowe zostały naruszone (art. 33 i 34).

2. Grupa Robocza Art. 29 już w październiku 2017 r. opracowała *ogólne* wytyczne dotyczące zgłaszania naruszeń ochrony danych, analizując odpowiednie sekcje RODO (Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, WP 250) (dalej „Wytyczne WP 250")[3]. Ze względu na swój charakter i termin wydania wytyczne te nie odnosiły się jednak wystarczająco szczegółowo do wszystkich praktycznych kwestii. W związku z tym pojawiła się potrzeba opracowania wytycznych *zorientowanych na praktykę, opartych na konkretnych przypadkach*, które wykorzystują doświadczenia zdobyte przez organy nadzorcze od czasu, gdy RODO zaczęło mieć zastosowanie.

[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".

[2] COM(2020) 264 final, z 24 czerwca 2020 r.

[3] Grupa Robocza Art. 29, WP250 rev.1, 6 lutego 2018 r., Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 – zatwierdzone przez EROD, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

3. Niniejszy dokument stanowi uzupełnienie Wytycznych WP 250 i odzwierciedla wspólne doświadczenia organów nadzorczych z EOG od czasu rozpoczęcia stosowania RODO. Jego celem jest pomoc administratorom danych w podejmowaniu decyzji o tym, jak postępować w przypadku naruszenia ochrony danych i jakie czynniki należy wziąć pod uwagę podczas oceny ryzyka.

4. Podejmując jakiekolwiek działania mające na celu zaradzenie naruszeniu, administrator i podmiot przetwarzający powinni w pierwszej kolejności potwierdzić jego wystąpienie. W art. 4 pkt 12 RODO „naruszenie ochrony danych osobowych" definiuje się jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

5. W swojej opinii 03/2014 na temat powiadamiania o przypadkach naruszenia[4] oraz w Wytycznych WP 250 Grupa Robocza Art. 29 wyjaśniła, że zgodnie z trzema powszechnie uznawanymi zasadami bezpieczeństwa naruszenia można podzielić na następujące kategorie:

   - „naruszenie dotyczące poufności danych" – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
   - „naruszenie dotyczące integralności danych" – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych;
   - „naruszenie dotyczące dostępności danych" – naruszenie, w rezultacie którego dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych[5].

6. Naruszenie może potencjalnie wywrzeć szereg negatywnych skutków dla osób fizycznych, które mogą skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub szkód niemajątkowych. W RODO wyjaśniono, że takie skutki mogą obejmować utratę kontroli nad własnymi danymi osobowymi, ograniczenie praw, dyskryminację, kradzież lub sfałszowanie tożsamości, stratę finansową, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia oraz naruszenie poufności danych osobowych chronionych tajemnicą zawodową. Mogą one również wiązać się z wszelkimi innymi znacznymi szkodami gospodarczymi lub społecznymi dla tych osób fizycznych. Jednym z najważniejszych obowiązków administratora danych jest ocena tych zagrożeń dla praw i wolności osób, których dane dotyczą, oraz wdrożenie odpowiednich środków technicznych i organizacyjnych w celu ich wyeliminowania.

7. W związku z tym w RODO wymaga się od administratora, aby:

   - dokumentował wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze[6];

---

[4] Grupa Robocza Art. 29, WP213, 25 marca 2014 r., Opinia 03/2014 na temat powiadamiania o przypadkach naruszenia danych osobowych, s. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4 .

[5] Zob. Wytyczne WP 250, s. 7. – Należy wziąć pod uwagę, że naruszenie ochrony danych może dotyczyć jednej kategorii lub kilku kategorii jednocześnie lub łącznie.

[6] Art. 33 ust. 5 RODO.

- zgłaszał przypadki naruszenia ochrony danych osobowych organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych[7];
- zawiadomił bez zbędnej zwłoki osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli takie naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych[8].

8. Naruszenia ochrony danych stanowią problem sam w sobie, ale mogą też być symptomami słabego, być może przestarzałego systemu bezpieczeństwa danych, mogą też wskazywać na słabości systemu, którymi należy się zająć. Ogólnie rzecz biorąc, zawsze lepiej jest zapobiegać naruszeniom ochrony danych, przygotowując się do nich z wyprzedzeniem, ponieważ niektóre ich konsekwencje są z natury rzeczy nieodwracalne. Zanim administrator będzie mógł *w pełni* ocenić ryzyko wynikające z naruszenia spowodowanego jakąś formą ataku, należy zidentyfikować pierwotną przyczynę problemu, aby stwierdzić, czy podatności, które spowodowały incydent, są nadal obecne i czy w związku z tym można je wykorzystać. W wielu przypadkach administrator jest w stanie stwierdzić, że incydent może spowodować ryzyko, a zatem należy go powiadomić. W innych przypadkach nie ma potrzeby odkładania zgłoszenia do czasu pełnej oceny ryzyka i skutków naruszenia, ponieważ pełna ocena ryzyka może być przeprowadzana równolegle ze zgłoszeniem, a uzyskane w ten sposób informacje mogą być przekazywane organowi nadzorczemu etapami bez zbędnej dalszej zwłoki[9].

9. Naruszenie należy zgłosić, gdy administrator jest zdania, że może ono spowodować ryzyko naruszenia praw i wolności osoby, której dane dotyczą. Administratorzy powinni dokonać tej oceny w momencie, gdy dowiadują się o naruszeniu. Administrator nie powinien czekać na szczegółową analizę kryminalistyczną i (wczesne) kroki zaradcze, zanim oceni, czy naruszenie ochrony danych prawdopodobnie spowoduje ryzyko, a zatem czy należy je zgłosić.

10. Jeżeli administrator sam oceni ryzyko jako mało prawdopodobne, ale okaże się, że ryzyko się zmaterializowało, właściwy organ nadzorczy może skorzystać ze swoich uprawnień naprawczych i może zastosować sankcje.

11. Każdy administrator i podmiot przetwarzający powinni mieć przygotowane plany i procedury postępowania w przypadku ewentualnego naruszenia ochrony danych. Organizacje powinny mieć jasno określoną hierarchię służbową i wyznaczyć osoby odpowiedzialne za określone aspekty procesu odzyskiwania danych.

12. Istotne znaczenie dla administratorów i podmiotów przetwarzających mają również szkolenia ich pracowników i podnoszenie wiedzy tych pracowników w zakresie ochrony danych osobowych, koncentrujące się na zarządzaniu naruszeniami ochrony danych osobowych (identyfikacja incydentu naruszenia ochrony danych osobowych i dalsze działania, jakie należy podjąć itp.). Szkolenie to powinno być regularnie powtarzane, w zależności od rodzaju działalności związanej z przetwarzaniem danych i wielkości administratora, z uwzględnieniem najnowszych trendów i alarmów związanych z cyberatakami lub innymi incydentami naruszającymi bezpieczeństwo.

13. Zasada rozliczalności i koncepcja uwzględnienia ochrony danych w fazie projektowania mogłyby obejmować analizę, która jest wykorzystywana przez administratora i podmiot przetwarzający we własnym

[7] Art. 33 ust. 1 RODO.

[8] Art. 34 ust. 1 RODO.

[9] Art. 33 ust. 4 RODO.

„Podręczniku postępowania w razie naruszenia ochrony danych osobowych", mającym na celu ustalenie faktów dotyczących każdego aspektu przetwarzania na każdym ważnym etapie operacji. Taki podręcznik przygotowany z wyprzedzeniem stanowiłby znacznie szybsze źródło informacji, które pozwoliłoby administratorom i podmiotom przetwarzającym zminimalizować ryzyko i wypełnić obowiązki bez zbędnej zwłoki. Dzięki temu w razie naruszenia ochrony danych osobowych pracownicy organizacji wiedzieliby, co robić, a sam incydent zostałby najprawdopodobniej szybciej opanowany niż w przypadku braku środków zaradczych lub planu.

14. Choć przedstawione poniżej przypadki są fikcyjne, opierają się na typowych przypadkach ze zbiorowego doświadczenia organu nadzorczego w zakresie zgłoszeń naruszeń ochrony danych. Przedstawione analizy odnoszą się wyraźnie do analizowanych przypadków, ale mają na celu zapewnienie pomocy administratorom danych w ocenie własnych naruszeń ochrony danych. Wszelkie zmiany w okolicznościach opisanych poniżej przypadków mogą skutkować innymi lub bardziej znaczącymi poziomami ryzyka, a tym samym wymagać innych lub dodatkowych środków. W niniejszych wytycznych przypadki uporządkowano według określonych kategorii naruszeń (np. ataki za pomocą oprogramowania szantażującego). W każdym przypadku, gdy mamy do czynienia z pewną kategorią naruszeń, konieczne jest zastosowanie pewnych środków łagodzących. Środki te nie muszą być powtarzane w każdym analizowanym przypadku należącym do tej samej kategorii naruszeń. W przypadkach należących do tej samej kategorii podano jedynie różnice. Dlatego czytelnik powinien zapoznać się ze wszystkimi przypadkami dotyczącymi danej kategorii naruszeń, aby zidentyfikować i rozróżnić wszystkie właściwe środki, które należy podjąć.

15. Wewnętrzna dokumentacja naruszenia jest obowiązkiem niezależnym od ryzyka związanego z naruszeniem i musi być sporządzana w każdym przypadku. Przedstawione poniżej przypadki próbują rzucić nieco światła na to, czy należy zgłosić naruszenie do organu nadzorczego i zawiadomić o nim osoby, których dane dotyczą.

2 OPROGRAMOWANIE SZANTAŻUJĄCE

16. Częstą przyczyną zgłoszenia naruszenia ochrony danych jest atak za pomocą oprogramowania szantażującego, którego ofiarą padł administrator danych. W takich przypadkach złośliwy kod szyfruje dane osobowe, a następnie sprawca ataku żąda od administratora danych okupu w zamian za kod deszyfrujący. Tego rodzaju atak można zwykle zaklasyfikować jako naruszenie dotyczące dostępności, ale często może też dojść do naruszenia dotyczącego poufności.

2.1 PRZYPADEK nr 01: Oprogramowanie szantażujące z prawidłowym tworzeniem kopii zapasowych i bez eksfiltracji

Systemy komputerowe małego przedsiębiorstwa produkcyjnej zostały narażone na atak za pomocą oprogramowania szantażującego, a dane przechowywane w tych systemach zostały zaszyfrowane. Administrator stosował szyfrowanie w stanie spoczynku, więc wszystkie dane, do których dostęp miało oprogramowanie szantażujące, były przechowywane w postaci zaszyfrowanej przy użyciu najnowocześniejszego algorytmu szyfrowania. Klucz deszyfrujący nie został naruszony podczas ataku, tzn. osoba atakująca nie miała do niego dostępu ani nie mogła go pośrednio wykorzystać. W rezultacie sprawca ataku miał dostęp tylko do zaszyfrowanych danych osobowych. W szczególności nie ucierpiał system poczty elektronicznej przedsiębiorstwa ani żadne systemy klienta, z których korzystano w celu uzyskania dostępu do tego systemu. Przedsiębiorstwo korzysta z wiedzy zewnętrznego przedsiębiorstwa zajmującego się cyberbezpieczeństwem w celu zbadania tego incydentu. Dostępne są dzienniki śledzące wszystkie przepływy danych opuszczających przedsiębiorstwo (w tym wychodzące wiadomości e-mail). Po przeanalizowaniu dzienników i danych zebranych przez systemy wykrywania wdrożone przez przedsiębiorstwo, w wyniku wewnętrznego dochodzenia prowadzonego przy wsparciu zewnętrznego przedsiębiorstwa zajmującego się cyberbezpieczeństwem ustalono *z całą pewnością*, że sprawca jedynie zaszyfrował dane, nie eksfiltrując ich. Dzienniki nie wykazują żadnego wypływu danych na zewnątrz w okresie, w którym miał miejsce atak. Dane osobowe, których dotyczyło naruszenie, odnosiły się do klientów i pracowników przedsiębiorstwa, w sumie kilkudziesięciu osób. Kopia zapasowa była łatwo dostępna, a dane zostały przywrócone kilka godzin po ataku. Naruszenie nie wpłynęło w żaden sposób na bieżącą działalność administratora. Nie było opóźnień w wypłatach dla pracowników ani w obsłudze zgłoszeń od klientów.

17. W tym przypadku z definicji „naruszenia ochrony danych osobowych” zrealizowano następujące elementy: naruszenie bezpieczeństwa doprowadziło do niezgodnej z prawem zmiany i nieuprawnionego dostępu do przechowywanych danych osobowych.

2.1.1 PRZYPADEK nr 01 – Środki zapobiegawcze i ocena ryzyka

18. Podobnie jak w przypadku wszystkich zagrożeń stwarzanych przez podmioty zewnętrzne, prawdopodobieństwo powodzenia ataku za pomocą oprogramowania szantażującego można drastycznie zmniejszyć, zwiększając bezpieczeństwo środowiska kontroli danych. Większości takich naruszeń można zapobiec, upewniając się, że podjęto odpowiednie organizacyjne, fizyczne i technologiczne środki bezpieczeństwa. Przykładem takich środków jest właściwe zarządzanie poprawkami oraz stosowanie odpowiedniego systemu wykrywania złośliwego oprogramowania. Posiadanie odpowiedniej i oddzielnej kopii zapasowej pomoże złagodzić skutki udanego ataku, jeśli do niego dojdzie. Ponadto program kształcenia, szkolenia i szerzenia wiedzy w zakresie bezpieczeństwa wśród pracowników (SETA) pomoże zapobiegać tego rodzaju atakom i je rozpoznawać. (Wykaz zalecanych środków można znaleźć w sekcji 2.5). Wśród tych środków najważniejsze jest odpowiednie zarządzanie poprawkami, które zapewnia aktualizację systemów i usuwanie wszystkich znanych luk w zabezpieczeniach wdrożonych systemów, ponieważ podczas większości ataków za pomocą oprogramowania szantażującego wykorzystuje się dobrze znane luki.

19. Oceniając ryzyko, administrator powinien zbadać naruszenie i zidentyfikować rodzaj złośliwego kodu, aby zrozumieć możliwe konsekwencje ataku. Wśród zagrożeń, które należy rozważyć, jest ryzyko, że dane zostały eksfiltrowane bez pozostawienia śladu w dziennikach systemów.

20. W tym przykładzie sprawca ataku miał dostęp do danych osobowych, a poufność zaszyfrowanego tekstu zawierającego dane osobowe w postaci zaszyfrowanej została naruszona. Wszelkie dane, które mogły zostać eksfiltrowane, nie mogą być jednak odczytane ani wykorzystane przez sprawcę, przynajmniej w chwili obecnej. Technika szyfrowania zastosowana przez administratora danych jest zgodna

z najnowszym stanem wiedzy. Klucz deszyfrujący nie został naruszony i przypuszczalnie nie mógł być również ustalony w inny sposób. W związku z tym ryzyko utraty poufności w odniesieniu do praw i wolności osób fizycznych jest ograniczone do minimum, chyba że postępy kryptoanalityczne sprawią, że zaszyfrowane dane staną się w przyszłości zrozumiałe.

21. Administrator danych powinien rozważyć ryzyko dla osób fizycznych wynikające z naruszenia[10]. W tym przypadku wydaje się, że ryzyko naruszenia praw i wolności osób, których dane dotyczą, wynika z braku dostępności danych osobowych, a poufność danych osobowych nie jest zagrożona[11]. W tym przykładzie negatywne skutki naruszenia złagodzono dość szybko po jego wystąpieniu. Posiadanie odpowiedniego systemu awaryjnego[12] sprawia, że skutki naruszenia są mniej dotkliwe, a administrator mógł je skutecznie wykorzystać w tym przypadku.

22. Jeżeli chodzi o dotkliwość konsekwencji dla osób, których dane dotyczą, można wskazać jedynie niewielkie konsekwencje, ponieważ dane będące przedmiotem ataku zostały przywrócone w ciągu kilku godzin, naruszenie nie spowodowało żadnych konsekwencji dla bieżącej działalności administratora i nie miało znaczącego wpływu na osoby, których dane dotyczą (np. płatności pracowników lub obsługa wniosków klientów).

2.1.2 PRZYPADEK nr 01 – Łagodzenie skutków i obowiązki

23. Bez kopii zapasowej administrator może podjąć niewiele działań naprawczych w związku z utratą danych osobowych, a dane muszą być gromadzone ponownie. W tym konkretnym przypadku skutki ataku można było jednak skutecznie ograniczyć, przywracając wszystkie zagrożone systemy do stanu, o którym wiadomo było, że nie zawierają złośliwego kodu, naprawiając luki w zabezpieczeniach i przywracając zaatakowane dane wkrótce po ataku. Bez kopii zapasowej dane zostają utracone, a dotkliwość ataku może wzrosnąć, ponieważ ryzyko lub wpływ na osoby fizyczne również mogą się zwiększyć.

24. Termin skutecznego przywrócenia danych z łatwo dostępnej kopii zapasowej jest kluczową zmienną podczas analizy naruszenia. Określenie odpowiednich ram czasowych na przywrócenie zagrożonych danych zależy od wyjątkowych okoliczności danego naruszenia. RODO stanowi, że naruszenie ochrony danych

---

[10]Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w „Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie »może powodować wysokie ryzyko« do celów rozporządzenia 2016/679, WP248 rev.01 – zatwierdzonych przez EROD, https://ec.europa.eu/newsroom/article29/items/611236, s. 9.

[11] Z technicznego punktu widzenia zaszyfrowanie danych wiąże się z „dostępem" do oryginalnych danych, a w przypadku oprogramowania szantażującego z usunięciem oryginału – kod oprogramowania szantażującego musi uzyskać dostęp do danych, aby je zaszyfrować i usunąć oryginalne dane. Sprawca ataku może wykonać kopię oryginału przed jego usunięciem, ale dane osobowe nie zawsze zostaną eksfiltrowane. W miarę postępu dochodzenia prowadzonego przez administratora mogą pojawić się nowe informacje, które spowodują zmianę tej oceny. Dostęp, który skutkuje niezgodnym z prawem zniszczeniem, utratą, zmodyfikowaniem, nieuprawnionym ujawnieniem danych osobowych lub zagrożeniem bezpieczeństwa osoby, której dane dotyczą, nawet bez interpretacji danych, może być równie dotkliwy jak dostęp z interpretacją danych osobowych.

[12] Procedury awaryjne powinny być uporządkowane, spójne i powtarzalne. Przykładami procedur awaryjnych są: metoda 3-2-1 oraz metoda „dziadek-ojciec-syn". Każdą metodę należy zawsze przetestować pod kątem skuteczności w zakresie pokrycia i w przypadku przywracania danych. Testowanie należy powtarzać w określonych odstępach czasu, a zwłaszcza w przypadku zmian w operacji przetwarzania lub jej uwarunkowań, aby zapewnić integralność systemu.

osobowych należy zgłosić bez zbędnej zwłoki, a jeśli jest to możliwe, nie później niż po 72 godzinach. Można zatem stwierdzić, że przekroczenie 72-godzinnego terminu jest niewskazane w każdym przypadku, ale w przypadku spraw o wysokim poziomie ryzyka nawet dotrzymanie tego terminu może być postrzegane jako niezadowalające.

25. W tym przypadku, po przeprowadzeniu szczegółowej oceny skutków i procesu reagowania na incydenty, administrator ustalił, że jest mało prawdopodobne, by naruszenie spowodowało ryzyko naruszenia praw i wolności osób fizycznych, dlatego nie ma potrzeby przekazywania informacji osobom, których dane dotyczą, ani zgłaszania naruszenia organowi nadzorczemu. Jak wszystkie naruszenia ochrony danych, należy je jednak udokumentować zgodnie z art. 33 ust. 5. Organizacja może również być zobowiązana (lub później zostanie zobowiązana przez organ nadzorczy) do aktualizacji i udoskonalenia swoich organizacyjnych i technicznych środków i procedur dotyczących bezpieczeństwa danych osobowych oraz środków i procedur ograniczających ryzyko. W ramach aktualizacji i działań naprawczych organizacja powinna dokładnie zbadać naruszenie oraz zidentyfikować jego przyczyny i metody zastosowane przez sprawcę, aby zapobiec podobnym zdarzeniom w przyszłości.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	X	X

2.2 PRZYPADEK nr 02: Oprogramowanie szantażujące bez prawidłowego tworzenia kopii zapasowych

Jeden z komputerów używanych przez przedsiębiorstwo rolnicze został narażony na atak za pomocą oprogramowania szantażującego, a jego dane zostały zaszyfrowane przez sprawcę ataku. Przedsiębiorstwo korzysta z wiedzy zewnętrznego przedsiębiorstwa zajmującego się cyberbezpieczeństwem w celu monitorowania swojej sieci. Dostępne są dzienniki śledzące wszystkie przepływy danych opuszczających przedsiębiorstwo (w tym wychodzące wiadomości e-mail). Po przeanalizowaniu dzienników i danych zebranych przez pozostałe systemy wykrywania, w ramach wewnętrznego dochodzenia prowadzonego przy wsparciu przedsiębiorstwa zajmującego się cyberbezpieczeństwem ustalono, że sprawca ataku jedynie zaszyfrował dane, nie dokonując ich eksfiltracji. Dzienniki nie wykazują żadnego wypływu danych na zewnątrz w okresie, w którym miał miejsce atak. Dane osobowe, których dotyczyło naruszenie, odnosiły się do pracowników i klientów przedsiębiorstwa, w sumie kilkudziesięciu osób. Nie dotyczyło to żadnych szczególnych kategorii danych. Nie była dostępna żadna kopia zapasowa w formie elektronicznej. Większość danych odtworzono z kopii zapasowych w formie papierowej. Przywracanie danych trwało 5 dni roboczych i spowodowało niewielkie opóźnienia w dostarczaniu zamówień do klientów.

2.2.1 PRZYPADEK nr 02 – Środki zapobiegawcze i ocena ryzyka

26. Administrator danych powinien był zastosować te same środki zapobiegawcze, o których mowa w części 2.1. oraz w sekcji 2.9. Główną różnicą w stosunku do poprzedniego przypadku jest brak elektronicznej kopii zapasowej oraz brak szyfrowania w stanie spoczynku. Prowadzi to do krytycznych różnic w kolejnych krokach.

27. Oceniając ryzyko, administrator powinien zbadać metodę infiltracji i zidentyfikować rodzaj złośliwego kodu, aby zrozumieć możliwe konsekwencje ataku. W tym przykładzie oprogramowanie szantażujące zaszyfrowało dane osobowe bez ich eksfiltracji. W rezultacie wydaje się, że ryzyko naruszenia praw i wolności osób, których dane dotyczą, wynika z braku dostępności danych osobowych, a poufność danych osobowych nie jest zagrożona. Dokładna analiza logów zapory sieciowej i jej implikacji jest niezbędna do

określenia ryzyka. Administrator powinien przedstawić na żądanie ustalenia faktyczne wynikające z tych badań.

28. Administrator musi pamiętać, że jeśli atak jest bardziej zaawansowany, złośliwe oprogramowanie może edytować pliki dziennika i usuwać ślady. Zatem – biorąc pod uwagę, że dzienniki nie są przekazywane ani replikowane do centralnego serwera dzienników – nawet po przeprowadzeniu dokładnego dochodzenia, w trakcie którego wykazano, że dane osobowe nie zostały eksfiltrowane przez sprawcę ataku administrator danych nie może stwierdzić, że brak wpisu w dzienniku dowodzi braku eksfiltracji, a zatem nie można całkowicie odrzucić prawdopodobieństwa naruszenia dotyczącego poufności.

29. Administrator powinien ocenić ryzyko tego naruszenia[13], jeżeli sprawca ataku uzyskał dostęp do danych. Podczas oceny ryzyka administrator danych powinien również wziąć pod uwagę charakter, wrażliwość, ilość i kontekst danych osobowych, których dotyczy naruszenie. W tym przypadku naruszenie nie dotyczy żadnych szczególnych kategorii danych osobowych, a ilość danych będących przedmiotem ataku i liczba poszkodowanych osób, których dane dotyczą, jest niewielka.

30. Zebranie dokładnych informacji o nieuprawnionym dostępie jest kluczowe dla określenia poziomu ryzyka i zapobieżenia nowemu lub kontynuowanemu atakowi. Gdyby dane skopiowano z bazy danych, byłoby to oczywiście czynnikiem zwiększającym ryzyko. W przypadku braku pewności co do szczegółów nieuprawnionego dostępu należy rozważyć gorszy scenariusz i odpowiednio ocenić ryzyko.

31. Brak zapasowej bazy danych można uznać za czynnik zwiększający ryzyko w zależności od dotkliwości konsekwencji dla osób, których dane dotyczą, wynikających z braku dostępności danych.

2.2.2 PRZYPADEK nr 02 – Łagodzenie skutków i obowiązki

32. Bez kopii zapasowej administrator może podjąć niewiele działań naprawczych w związku z utratą danych osobowych, a dane muszą być gromadzone ponownie, chyba że dostępne jest inne źródło (np. e-maile z potwierdzeniem zamówienia). Bez kopii zapasowej dane mogą zostać utracone, a dotkliwość tej sytuacji będzie zależeć od skutków dla osób fizycznych.

33. Przywrócenie danych nie powinno okazać się zbyt problematyczne[14], jeśli dane są nadal dostępne w formie papierowej, jednak ze względu na brak elektronicznej kopii zapasowej bazy danych, powiadomienie organu nadzorczego uważa się za konieczne, ponieważ przywrócenie danych zajęło trochę czasu i może spowodować pewne opóźnienia w dostarczaniu zamówień do klientów, a znaczna ilość metadanych (np. logi, znaczniki czasu) może nie być możliwa do odzyskania.

34. Zawiadamianie osób, których dane dotyczą, o naruszeniu może również zależeć od długości okresu niedostępności danych osobowych oraz trudności, jakie może to spowodować w działalności administratora (np. opóźnienia w przekazywaniu płatności pracowników). W związku z tym, że takie opóźnienia w płatnościach i dostawach mogą prowadzić do strat finansowych dla osób, których dane zostały naruszone, można również stwierdzić, że naruszenie prawdopodobnie wiąże się z wysokim ryzykiem. Nie można też

[13] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

[14] Będzie to zależało od złożoności i struktury danych osobowych. W najbardziej złożonych przypadkach przywrócenie integralności danych, spójności z metadanymi, zapewnienie właściwych relacji w strukturach danych oraz sprawdzenie prawidłowości danych może wymagać znacznych zasobów i wysiłku.

uniknąć informowania osób, których dane dotyczą, jeśli ich udział jest konieczny do przywrócenia zaszyfrowanych danych.

35. Ten przypadek służy jako przykład ataku za pomocą oprogramowania szantażującego, który stwarza ryzyko naruszenia praw i wolności osób, których dane dotyczą, ale nie osiąga poziomu wysokiego ryzyka. Należy go udokumentować zgodnie z art. 33 ust. 5 i zgłosić organowi nadzorczemu zgodnie z art. 33 ust. 1. Organizacja może również być zobowiązana (lub zostanie zobowiązana przez organ nadzorczy) do aktualizacji i udoskonalenia swoich organizacyjnych i technicznych środków i procedur dotyczących bezpieczeństwa danych osobowych oraz środków i procedur ograniczających ryzyko.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	X

2.3 PRZYPADEK nr 03: Oprogramowanie szantażujące z kopią zapasową i bez eksfiltracji w szpitalu

System informatyczny szpitala/ośrodka opieki zdrowotnej został narażony na atak za pomocą oprogramowania szantażującego, w wyniku którego znaczna część danych została zaszyfrowana przez sprawcę ataku. Przedsiębiorstwo korzysta z wiedzy zewnętrznego przedsiębiorstwa zajmującego się cyberbezpieczeństwem w celu monitorowania swojej sieci. Dostępne są dzienniki śledzące wszystkie przepływy danych opuszczających przedsiębiorstwo (w tym wychodzące wiadomości e-mail). Po przeanalizowaniu dzienników i danych zebranych przez pozostałe systemy wykrywania, w ramach wewnętrznego dochodzenia prowadzonego przy wsparciu przedsiębiorstwa zajmującego się cyberbezpieczeństwem ustalono, że sprawca ataku jedynie zaszyfrował dane, nie dokonując ich eksfiltracji. Dzienniki nie wykazują żadnego wypływu danych na zewnątrz w okresie, w którym miał miejsce atak. Dane osobowe, których dotyczyło naruszenie, odnosiły się do pracowników i pacjentów, czyli tysięcy osób. Kopie zapasowe były dostępne w formie elektronicznej. Większość danych udało się przywrócić, ale operacja ta trwała 2 dni robocze i doprowadziła do znacznych opóźnień w leczeniu pacjentów – operacje zostały odwołane/przełożone, a także do obniżenia poziomu usług ze względu na niedostępność systemów.

2.3.1 PRZYPADEK nr 03 – Środki zapobiegawcze i ocena ryzyka

36. Administrator danych powinien był zastosować te same środki zapobiegawcze, o których mowa w części 2.1. oraz w sekcji 2.5. Główną różnicą w stosunku do poprzedniego przypadku jest wysoka skala skutków dla znacznej części osób, których dane dotyczą[15].

37. Ilość danych będących przedmiotem ataku i liczba poszkodowanych osób, których dane dotyczą, są duże, ponieważ szpitale zwykle przetwarzają duże ilości danych. Niedostępność danych w dużym stopniu wpływa na znaczną część osób, których dane dotyczą. Ponadto istnieje ryzyko szczątkowe o wysokim stopniu szkodliwości dla poufności danych pacjentów.

[15] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

38. Istotne są: rodzaj naruszenia, charakter, wrażliwość i ilość danych osobowych, których dotyczyło naruszenie. Nawet jeśli istniała kopia zapasowa danych i można było je przywrócić w ciągu kilku dni, nadal istnieje wysokie ryzyko ze względu na dotkliwość konsekwencji dla osób, których dane dotyczą, wynikających z braku dostępności danych w momencie ataku i w następnych dniach.

2.3.2 PRZYPADEK nr 03 – Łagodzenie skutków i obowiązki

39. Zgłoszenie organowi nadzorczemu uważa się za konieczne, ponieważ w grę wchodzą szczególne kategorie danych osobowych, a przywrócenie danych mogłoby zająć dużo czasu, powodując poważne opóźnienia w opiece nad pacjentami. Poinformowanie osób, których dane dotyczą, o naruszeniu jest konieczne ze względu na skutki dla pacjentów, nawet po przywróceniu zaszyfrowanych danych. Chociaż dane dotyczące wszystkich pacjentów leczonych w szpitalu w ciągu ostatnich lat zostały zaszyfrowane, skutki naruszenia dotknęły tylko tych pacjentów, którzy mieli być leczeni w szpitalu w czasie, gdy system komputerowy był niedostępny. Administrator powinien bezpośrednio zawiadomić tych pacjentów o naruszeniu ochrony danych. Bezpośrednie powiadomienie pozostałych pacjentów, z których niektórzy mogli nie przebywać w szpitalu od ponad dwudziestu lat, może nie być wymagane ze względu na wyjątek określony w art. 34 ust. 3 lit. c). W takim przypadku wydany zostaje publiczny komunikat[16] lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. W tym przypadku szpital powinien upublicznić informację o ataku za pomocą oprogramowania szantażującego i jego skutkach.

40. Ten przypadek służy jako przykład ataku za pomocą oprogramowania szantażującego, który stwarza wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Należy go udokumentować zgodnie z art. 33 ust. 5 i zgłosić organowi nadzorczemu zgodnie z art. 33 ust. 1, a także zawiadomić o zdarzeniu osoby, których dane dotyczą, zgodnie z art. 34 ust. 1. Organizacja może również być zobowiązana do aktualizacji i udoskonalenia swoich organizacyjnych i technicznych środków i procedur dotyczących bezpieczeństwa danych osobowych oraz środków i procedur ograniczania ryzyka.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	**Zgłoszenie organowi nadzorczemu**	**Zawiadomienie osób, których dane dotyczą**
✓	✓	✓

2.4 PRZYPADEK nr 04: Oprogramowanie szantażujące bez kopii zapasowej i z eksfiltracją

[16] W motywie 86 RODO wyjaśniono, że „[i]nformacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania. Na przykład potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie”.

Serwer przedsiębiorstwa zajmującego się transportem publicznym został narażony na atak za pomocą oprogramowania szantażującego, a jego dane zostały zaszyfrowane przez sprawcę ataku. Zgodnie z ustaleniami z wewnętrznego dochodzenia sprawca nie tylko zaszyfrował dane, ale także dokonał ich eksfiltracji. Naruszone zostały dane osobowe klientów i pracowników, a także kilku tysięcy osób korzystających z usług przedsiębiorstwa (np. kupujących bilety online). Poza podstawowymi danymi dotyczącymi tożsamości naruszenie dotyczyło numerów dowodów tożsamości i danych finansowych, takich jak dane kart kredytowych. Istniała zapasowa baza danych, ale ona również została zaszyfrowana przez sprawcę ataku.

2.4.1 PRZYPADEK nr 04 – Środki zapobiegawcze i ocena ryzyka

41. Administrator danych powinien był zastosować te same środki zapobiegawcze, o których mowa w części 2.1. oraz w sekcji 2.5. Chociaż istniała kopia zapasowa, ona także została objęta atakiem. Już samo to rozwiązanie budzi wątpliwości co do jakości wcześniejszych środków bezpieczeństwa informatycznego stosowanych przez administratora i powinno zostać dokładniej przeanalizowane podczas dochodzenia, ponieważ w dobrze zaprojektowanym systemie tworzenia kopii zapasowych tworzy się kilka kopii zapasowych, które muszą być bezpiecznie przechowywane bez dostępu z głównego systemu, w przeciwnym razie mogą zostać narażone na ten sam atak. Ponadto ataki za pomocą oprogramowania szantażującego mogą pozostawać niewykryte przez wiele dni, a sprawca może powoli szyfrować rzadko używane dane. Może to spowodować, że takie kopie zapasowe staną się bezużyteczne, dlatego kopie zapasowe powinny być tworzone okresowo i izolowane. Zwiększyłoby to prawdopodobieństwo odzyskania danych, choć wiązałoby się z większą ich utratą.

42. Naruszenie to dotyczy nie tylko dostępności danych, ale także ich poufności, ponieważ osoba atakująca mogła zmodyfikować lub skopiować dane z serwera. W związku z tym ten rodzaj naruszenia może powodować wysokie ryzyko[17].

43. Charakter, wrażliwość i ilość danych osobowych dodatkowo zwiększają ryzyko, ponieważ liczba osób, których te dane dotyczą, jest wysoka, podobnie jak ogólna ilość danych osobowych, będących przedmiotem ataku. Poza podstawowymi danymi dotyczącymi tożsamości, w grę wchodzą także dokumenty tożsamości i dane finansowe, takie jak dane kart kredytowych. Naruszenie ochrony danych dotyczące tych rodzajów danych stanowi samo w sobie wysokie ryzyko, a jeśli są one przetwarzane razem, mogą zostać wykorzystane m.in. do kradzieży tożsamości lub nadużyć finansowych.

44. Z powodu błędnej logiki serwera lub kontroli organizacyjnych oprogramowanie szantażujące zaatakowało pliki kopii zapasowych, co uniemożliwiło przywrócenie danych i zwiększyło ryzyko.

45. To naruszenie ochrony danych stanowi wysokie ryzyko dla praw i wolności osób fizycznych, ponieważ może prowadzić zarówno do szkód materialnych (np. strat finansowych, gdyż naruszone zostały dane karty kredytowej), jak i niematerialnych (np. kradzieży tożsamości lub nadużyć finansowych, ponieważ naruszone zostały dane z dowodu tożsamości).

2.4.2 PRZYPADEK nr 04 – Łagodzenie skutków i obowiązki

46. Niezbędne jest zawiadomienie osób, których dane dotyczą, aby mogły one podjąć kroki niezbędne do uniknięcia szkód materialnych (np. zablokować karty kredytowe).

[17] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko” można znaleźć w przypisie 10 powyżej.

47. Oprócz udokumentowania naruszenia zgodnie z art. 33 ust. 5, w tym przypadku obowiązkowe jest również zgłoszenie naruszenia organowi nadzorczemu (art. 33 ust. 1), a administrator jest również zobowiązany do zawiadomienia o naruszeniu osób, których dane dotyczą (art. 34 ust. 1). To ostatnie może być przeprowadzane indywidualnie, ale w przypadku osób, których dane kontaktowe nie są dostępne, administrator powinien zrobić to publicznie, pod warunkiem, że takie powiadomienie nie spowoduje dodatkowych negatywnych konsekwencji dla osób, których dane dotyczą, np. w formie powiadomienia na swojej stronie internetowej. W tym ostatnim przypadku wymagany jest precyzyjny i jasny komunikat, umieszczony w widocznym miejscu na stronie głównej administratora, z dokładnymi odniesieniami do odpowiednich przepisów RODO. Organizacja może również być zobowiązana do aktualizacji i udoskonalenia swoich organizacyjnych i technicznych środków i procedur dotyczących bezpieczeństwa danych osobowych oraz środków i procedur ograniczania ryzyka.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	✓

2.5 Środki organizacyjne i techniczne służące zapobieganiu skutkom ataków za pomocą oprogramowania szantażującego i ich łagodzeniu

48. Fakt, że atak za pomocą oprogramowania szantażującego mógł mieć miejsce, jest zwykle oznaką istnienia co najmniej jednej luki w systemie administratora. Dotyczy to również przypadków oprogramowania szantażującego, w których dane osobowe zostały zaszyfrowane, ale nie uległy eksfiltracji. Niezależnie od wyniku i konsekwencji ataku, nie sposób przecenić znaczenia kompleksowej oceny systemu bezpieczeństwa danych – ze szczególnym uwzględnieniem bezpieczeństwa informatycznego. Zidentyfikowane słabości i luki w zabezpieczeniach należy udokumentować i bezzwłocznie usunąć.

49. Zalecane środki:

(Lista poniższych środków nie jest w żadnym wypadku wyłączna ani wyczerpująca. Celem jest raczej przedstawienie pomysłów na zapobieganie atakom i możliwych rozwiązań. Każda czynność przetwarzania danych jest inna, dlatego administrator powinien podjąć decyzję, które środki najbardziej pasują do danej sytuacji.)

- aktualizowanie oprogramowania układowego, systemu operacyjnego i oprogramowania użytkowego na serwerach, komputerach klienckich, aktywnych składnikach sieci i wszelkich innych urządzeniach w tej samej sieci LAN (w tym urządzeniach Wi-Fi). Zapewnienie odpowiednich środków bezpieczeństwa informatycznego, upewnienie się, że są one skuteczne oraz ich regularne aktualizowanie w przypadku zmiany lub rozwoju procesów lub okoliczności. Obejmuje to prowadzenie szczegółowych dzienników, w których zapisywane są informacje o tym, jakie poprawki zastosowano w danym znaczniku czasu;
- projektowanie i organizowanie systemów przetwarzania i infrastruktury w celu segmentacji lub izolacji systemów danych i sieci, aby uniknąć rozprzestrzeniania się złośliwego oprogramowania wewnątrz organizacji i do systemów zewnętrznych;
- istnienie aktualnej, bezpiecznej i sprawdzonej procedury tworzenia kopii zapasowych. Nośniki do średnio- i długoterminowego tworzenia kopii zapasowych powinny być przechowywane oddzielnie od magazynu danych operacyjnych i poza zasięgiem osób trzecich, nawet w przypadku udanego ataku (np. codzienna przyrostowa kopia zapasowa i cotygodniowa pełna kopia zapasowa);
- posiadanie/uzyskanie odpowiedniego, aktualnego, skutecznego i zintegrowanego programu chroniącego przed złośliwym oprogramowaniem;

- posiadanie odpowiedniej, aktualnej, skutecznej i zintegrowanej zapory sieciowej oraz systemu wykrywania włamań i zapobiegania im. Kierowanie ruchu sieciowego przez zaporę sieciową / system wykrywania włamań, nawet w przypadku pracy z domu lub pracy mobilnej (np. poprzez korzystanie z połączeń VPN z organizacyjnymi mechanizmami bezpieczeństwa podczas łączenia się z internetem);
- szkolenie pracowników w zakresie metod rozpoznawania ataków informatycznych i zapobiegania tym atakom. Administrator powinien zapewnić środki pozwalające ustalić, czy wiadomości e-mail i wiadomości otrzymane za pomocą innych środków komunikacji są autentyczne i godne zaufania. Pracownicy powinni zostać przeszkoleni w zakresie rozpoznawania, kiedy doszło do takiego ataku, sposobów umieszczenia punktu końcowego poza siecią oraz obowiązku natychmiastowego zgłoszenia tego faktu specjaliście ds. zabezpieczeń;
- podkreślenie potrzeby identyfikacji typu złośliwego kodu w celu poznania konsekwencji ataku i znalezienia odpowiednich środków zmniejszających ryzyko. Jeśli atak za pomocą oprogramowania szantażującego się powiódł i nie ma kopii zapasowej, w celu odzyskania danych można skorzystać z dostępnych narzędzi, takich jak te opracowane w ramach projektu „no more ransom" (nomoreransom.org). Jeśli jednak dostępna jest bezpieczna kopia zapasowa, zalecane jest przywrócenie danych z tej kopii;
- przekazywanie lub replikacja wszystkich dzienników do centralnego serwera dzienników (z ewentualnym podpisywaniem lub kryptograficznym znakowaniem czasowym wpisów dzienników);
- silne szyfrowanie i uwierzytelnianie wielopoziomowe, w szczególności w przypadku dostępu administracyjnego do systemów informatycznych, odpowiednie zarządzanie kluczami i hasłami;
- regularne testowanie podatności na zagrożenia i testy penetracyjne;
- powołanie w organizacji zespołu reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) lub zespołu reagowania na incydenty komputerowe (CERT) albo przyłączenie się do zbiorowego CSIRT/CERT. Opracowanie planu reagowania na incydenty, planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej oraz planu ciągłości działania i upewnienie się, że są one dokładnie przetestowane;
- przy ocenie środków zaradczych – analiza ryzyka powinna podlegać przeglądowi, być testowana i aktualizowana.

3 ATAKI POLEGAJĄCE NA EKSFILTRACJI DANYCH

50. Ataki wykorzystujące luki w usługach oferowanych przez administratora osobom trzecim przez internet, np. ataki polegające na wstrzyknięciu (np. wstrzykiwaniu kodu SQL, przechodzeniu przez ścieżki), ataki na strony internetowe i podobne metody, mogą przypominać ataki za pomocą oprogramowania szantażującego, ponieważ zagrożenie wynika z działania nieupoważnionej osoby trzeciej, ale ataki te zazwyczaj mają na celu skopiowanie, eksfiltrację i wykorzystanie danych osobowych do złych celów. Są to zatem głównie przypadki naruszenia dotyczącego poufności i ewentualnie integralności danych. Jednocześnie, jeśli administrator jest świadomy cech charakterystycznych tego rodzaju naruszeń, ma do dyspozycji wiele środków, które mogą znacznie zmniejszyć ryzyko udanego przeprowadzenia ataku.

3.1 PRZYPADEK nr 05: Eksfiltracja ze strony internetowej danych dotyczących podań o pracę

Agencja pośrednictwa pracy padła ofiarą cyberataku, w wyniku którego na jej stronie internetowej został umieszczony złośliwy kod. Ten złośliwy kod sprawił, że dane osobowe przesłane za pośrednictwem internetowych formularzy podań o pracę i przechowywane na serwerze internetowym stały się dostępne dla nieupoważnionej osoby (osób). Możliwe, że naruszenie dotyczyło 213 takich formularzy; po przeanalizowaniu danych, które zostały naruszone, stwierdzono, że naruszenie nie dotyczyło żadnych szczególnych kategorii danych. Zainstalowane złośliwe oprogramowanie posiadało funkcje, które pozwoliły sprawcy ataku na usunięcie wszelkich historii eksfiltracji, a także umożliwiły monitorowanie przetwarzania danych na serwerze i przechwytywanie danych osobowych. Oprogramowanie wykryto dopiero miesiąc po jego zainstalowaniu.

3.1.1 PRZYPADEK nr 05 – Środki zapobiegawcze i ocena ryzyka

51. Bezpieczeństwo środowiska administratora danych jest niezwykle ważne, gdyż większości takich naruszeń można zapobiec, dbając o to, by wszystkie systemy były stale aktualizowane, dane wrażliwe szyfrowane, a aplikacje tworzone zgodnie z wysokimi standardami bezpieczeństwa, takimi jak silne uwierzytelnianie, środki przeciwdziałające atakom siłowym, ataki, „anulowanie" lub „sanityzacja"[18] danych wprowadzanych przez użytkownika itp. Wymagane są również okresowe audyty bezpieczeństwa informatycznego, oceny luk w zabezpieczeniach i testy penetracyjne, aby zawczasu wykrywać tego rodzaju luki i je usuwać. W tym konkretnym przypadku, narzędzia monitorujące integralność plików w środowisku produkcyjnym mogły pomóc w wykryciu wstrzyknięcia kodu. (Wykaz zalecanych środków można znaleźć w sekcji 3.7).

52. Administrator powinien zawsze rozpoczynać badanie naruszenia od określenia rodzaju ataku i jego metod, aby ocenić, jakie środki należy zastosować. Aby działać szybko i skutecznie, administrator danych powinien dysponować planem reagowania na incydenty, który określa szybkie i niezbędne kroki w celu przejęcia kontroli nad incydentem. W tym konkretnym przypadku rodzaj naruszenia stanowił czynnik zwiększający ryzyko, ponieważ nie tylko ograniczono poufność danych, ale infiltrator dysponował także środkami umożliwiającymi wprowadzenie zmian w systemie, więc integralność danych również stała się wątpliwa.

53. Należy ocenić charakter, wrażliwość i ilość danych osobowych, których dotyczyło naruszenie, aby ustalić, w jakim stopniu naruszenie wpłynęło na osoby, których dane dotyczą. Mimo że nie naruszono żadnych szczególnych kategorii danych osobowych, dane, do których uzyskano dostęp, zawierają znaczące informacje o osobach z formularzy internetowych, a takie dane mogą zostać wykorzystane niewłaściwie na wiele różnych sposobów (kierowanie niechcianych reklam, kradzież tożsamości itp.), tak więc dotkliwość konsekwencji powinna zwiększać ryzyko naruszenia praw i wolności osób, których dane dotyczą[19].

3.1.2 PRZYPADEK nr 05 – Łagodzenie skutków i obowiązki

54. Jeśli to możliwe, po rozwiązaniu problemu należy porównać bazę danych z bazą przechowywaną w bezpiecznej kopii zapasowej. Doświadczenia wyniesione z naruszenia powinny zostać wykorzystane do

[18] Anulowanie lub sanityzacja danych wprowadzanych przez użytkownika jest formą walidacji danych wejściowych, która zapewnia, że do systemu informatycznego wprowadzane są tylko prawidłowo sformatowane dane.

[19] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

aktualizacji infrastruktury informatycznej. Administrator danych powinien przywrócić wszystkie systemy informatyczne, których dotyczy naruszenie, do znanego, czystego stanu, naprawić luki w zabezpieczeniach i wdrożyć nowe środki bezpieczeństwa, aby uniknąć podobnych naruszeń danych w przyszłości, np. kontrole integralności plików i audyty bezpieczeństwa. Jeśli dane osobowe zostały nie tylko eksfiltrowane, ale także usunięte, administrator musi podejmować systematyczne działania w celu odzyskania danych osobowych w stanie, w jakim znajdowały się przed naruszeniem. Konieczne może być zastosowanie pełnych kopii zapasowych, zmian przyrostowych, a następnie ewentualne ponowne uruchomienie przetwarzania od czasu ostatniej przyrostowej kopii zapasowej – co wymaga, aby administrator był w stanie odtworzyć zmiany dokonane od czasu ostatniej kopii zapasowej. Może to wymagać od administratora posiadania systemu zaprojektowanego tak, by zachowywał dzienne pliki wejściowe na wypadek konieczności ich ponownego przetworzenia, a także wymaga solidnej metody przechowywania i odpowiedniej polityki przechowywania.

55. W świetle powyższego, ponieważ naruszenie prawdopodobnie spowoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych, osoby, których dane dotyczą, powinny zostać o nim zdecydowanie poinformowane (art. 34 ust. 1), co oczywiście oznacza, że odpowiedni organ nadzorczy również powinien zostać zaangażowany w formie zgłoszenia naruszenia ochrony danych. Dokumentowanie naruszenia jest obowiązkowe zgodnie z art. 33 ust. 5 RODO i ułatwia ocenę sytuacji.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	✓

3.2 PRZYPADEK nr 06: Eksfiltracja zahaszowanego hasła ze strony internetowej

Wykorzystano lukę w zabezpieczeniach do wstrzyknięcia kodu SQL w celu uzyskania dostępu do bazy danych serwera strony internetowej poświęconej gotowaniu. Użytkownicy mogli wybierać tylko dowolne pseudonimy jako nazwy użytkownika. Odradzano używanie do tego celu adresów e-mail. Hasła przechowywane w bazie danych były haszowane za pomocą silnego algorytmu, a ciąg inicjujący (ang. salt) nie został naruszony. Naruszone dane: zahaszowane hasła 1 200 użytkowników. Ze względów bezpieczeństwa administrator zawiadomił osoby, których dane dotyczą, o naruszeniu za pośrednictwem poczty elektronicznej i poprosił je o zmianę haseł, zwłaszcza jeśli to samo hasło było używane do innych usług.

3.2.1 PRZYPADEK nr 06 – Środki zapobiegawcze i ocena ryzyka

56. W tym konkretnym przypadku poufność danych jest zagrożona, ale hasła w bazie danych zostały zahaszowane przy użyciu nowoczesnej metody, co zmniejszyłoby ryzyko związane z charakterem, wrażliwością i ilością danych osobowych. Ten przypadek nie stanowi zagrożenia dla praw i wolności osób, których dane dotyczą.

57. Ponadto nie naruszono żadnych informacji kontaktowych (np. adresów e-mail lub numerów telefonów) osób, których dane dotyczą, co oznacza, że nie istnieje znaczące ryzyko, że osoby, których dane dotyczą, staną się celem prób oszustwa (np. otrzymywania wiadomości e-mail typu phishing lub oszukańczych wiadomości tekstowych i połączeń telefonicznych). Nie dotyczyło to żadnych szczególnych kategorii danych osobowych.

58. Niektóre nazwy użytkowników można by uznać za dane osobowe, ale tematyka strony internetowej nie pozwala na negatywne skojarzenia. Należy jednak zauważyć, że ocena ryzyka może ulec zmianie[20], jeśli rodzaj strony internetowej i dane, do których dostęp jest możliwy, mogą ujawniać szczególne kategorie danych osobowych (np. strona partii politycznej lub związku zawodowego). Zastosowanie najnowocześniejszego szyfrowania może złagodzić negatywne skutki naruszenia. Zapewnienie ograniczonej liczby prób logowania uniemożliwi udane ataki siłowe, co w znacznym stopniu zmniejszy ryzyko związane z tym, że sprawcy ataku znają już nazwy użytkowników.

3.2.2 PRZYPADEK nr 06 – Łagodzenie skutków i obowiązki

59. W niektórych przypadkach zawiadomienie osób, których dane dotyczą, można uznać za czynnik ograniczający ryzyko, ponieważ osoby te są w stanie podjąć kroki niezbędne do uniknięcia dalszych szkód związanych z naruszeniem, np. zmienić hasło. W tym przypadku zawiadomienie nie było obowiązkowe, ale w wielu przypadkach można je uznać za dobrą praktykę.

60. Administrator danych powinien naprawić luki w zabezpieczeniach i wdrożyć nowe środki bezpieczeństwa, aby uniknąć podobnych naruszeń danych w przyszłości, np. systematyczne audyty bezpieczeństwa na stronie internetowej.

61. Naruszenie powinno być udokumentowane zgodnie z art. 33 ust. 5, ale nie ma potrzeby zgłaszania go ani zawiadamiania o nim.

62. Ponadto zdecydowanie zaleca się zawiadamianie osób, których dane dotyczą, o naruszeniu dotyczącym haseł, nawet jeśli hasła były przechowywane z użyciem ciągu inicjującego, z wykorzystaniem algorytmu zgodnego z najnowszymi standardami. Preferowane jest stosowanie metod uwierzytelniania, które eliminują konieczność przetwarzania haseł po stronie serwera. Osoby, których dane dotyczą, powinny mieć możliwość podjęcia odpowiednich działań w odniesieniu do własnych haseł.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	X	X

3.3 PRZYPADEK nr 07: Atak typu „credential stuffing” na witrynę bankową

[20] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko” można znaleźć w przypisie 10 powyżej.

Pewien bank ucierpiał w wyniku cyberataku na jedną ze swoich stron internetowych poświęconych bankowości internetowej. Celem ataku było wyliczenie wszystkich możliwych identyfikatorów użytkowników logujących się przy użyciu ustalonego trywialnego hasła. Hasła składają się z 8 cyfr. Z powodu luki w zabezpieczeniach strony internetowej w niektórych przypadkach informacje dotyczące osób, których dane dotyczą (imię, nazwisko, płeć, data i miejsce urodzenia, numer identyfikacji podatkowej, kody identyfikacyjne użytkownika), wyciekły do sprawcy ataku, nawet jeśli użyte hasło nie było poprawne lub rachunek bankowy nie był już aktywny. Atak dotknął około 100 000 osób, których dane dotyczą. Spośród nich sprawca ataku z powodzeniem zalogował się na ok. 2 000 kont, do których użyto wypróbowanego przez niego trywialnego hasła. Po fakcie administrator był w stanie zidentyfikować wszystkie nieuprawnione próby logowania. Administrator mógł potwierdzić, że zgodnie z wynikami kontroli przeciwko nadużyciom finansowym w czasie ataku na te konta nie dokonano żadnych transakcji. Bank był świadomy naruszenia ochrony danych, ponieważ jego centrum monitorowania bezpieczeństwa wykryło dużą liczbę żądań logowania skierowanych na stronę internetową. W odpowiedzi administrator zablokował możliwość zalogowania się na stronie internetowej poprzez jej wyłączenie i wymusił resetowanie haseł na zagrożonych kontach. Administrator zawiadomił o naruszeniu tylko tych użytkowników, których konta zostały naruszone, tj. użytkowników, których hasła zostały naruszone lub których dane zostały ujawnione.

3.3.1 PRZYPADEK nr 07 – Środki zapobiegawcze i ocena ryzyka

63. Należy wspomnieć, że na administratorach przetwarzających dane o charakterze wysoce osobistym[21] spoczywa większa odpowiedzialność za zapewnienie odpowiedniego bezpieczeństwa danych, np. posiadanie centrum monitorowania bezpieczeństwa oraz innych środków zapobiegania incydentom, wykrywania ich i reagowania na nie. Niespełnienie tych wyższych standardów z pewnością spowoduje podjęcie poważniejszych kroków podczas dochodzenia prowadzonego przez organ nadzorczy.

64. Naruszenie dotyczy danych finansowych, a nie tylko informacji dotyczących tożsamości i identyfikatorów użytkowników, co czyni je szczególnie poważnym. Liczba osób, których dotyczy naruszenie, jest wysoka.

65. Fakt, że do naruszenia mogło dojść w tak wrażliwym środowisku świadczy o istotnych lukach w bezpieczeństwie danych w systemie administratora i może wskazywać na moment, w którym przegląd i aktualizacja środków są „konieczne" zgodnie z art. 24 ust. 1, art. 25 ust. 1 i art. 32 ust. 1 RODO. Naruszone dane pozwalają na jednoznaczną identyfikację osób, których dane dotyczą, i zawierają inne informacje na ich temat (w tym płeć, datę i miejsce urodzenia), ponadto mogą być wykorzystane przez atakującego do odgadnięcia haseł klientów lub przeprowadzenia kampanii spear phishingowej skierowanej do klientów banku.

66. Z tych powodów uznano, że naruszenie ochrony danych prawdopodobnie spowoduje wysokie ryzyko naruszenia praw i wolności wszystkich osób, których dane dotyczą[22]. W związku z tym możliwe jest

[21] Np. informacje o metodach płatności osób, których dane dotyczą, takie jak numery kart, rachunki bankowe, płatności online, listy płac, wyciągi bankowe, analizy ekonomiczne lub inne informacje, które mogą ujawnić informacje ekonomiczne o osobach, których dane dotyczą.

[22] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

wystąpienie szkód materialnych (np. strat finansowych) i niematerialnych (np. kradzieży tożsamości lub oszustwa).

3.3.2 PRZYPADEK nr 07 – Łagodzenie skutków i obowiązki

67. Środki podjęte przez administratora wymienione w opisie przypadku są odpowiednie. W następstwie naruszenia naprawił on również luki w zabezpieczeniach na stronie internetowej i podjął inne kroki w celu zapobieżenia podobnym naruszeniom danych w przyszłości, takie jak dodanie dwuskładnikowego uwierzytelniania do danej strony internetowej i przejście na silne uwierzytelnianie klienta.

68. Udokumentowanie naruszenia zgodnie z art. 33 ust. 5 RODO i zgłoszenie go organowi nadzorczemu nie jest opcjonalne w tym scenariuszu. Ponadto administrator danych powinien zawiadomić wszystkie 100 000 osób, których dane dotyczą (w tym osoby, których konta nie zostały naruszone), zgodnie z art. 34 RODO.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	✓

3.4 Środki organizacyjne i techniczne służące zapobieganiu skutkom ataków hakerów i ich łagodzeniu

69. Podobnie jak w przypadku ataków za pomocą oprogramowania szantażującego, niezależnie od wyniku i konsekwencji ataku, ponowna ocena bezpieczeństwa informatycznego jest obowiązkowa dla administratorów w podobnych przypadkach.

70. Zalecane środki[23]:

(*Lista poniższych środków nie jest w żadnym wypadku wyłączna ani wyczerpująca. Celem jest raczej przedstawienie pomysłów na zapobieganie atakom i możliwych rozwiązań. Każda czynność przetwarzania danych jest inna, dlatego administrator powinien podjąć decyzję, które środki najbardziej pasują do danej sytuacji*.)

- najnowocześniejsze szyfrowanie i zarządzanie kluczami, zwłaszcza w przypadku przetwarzania haseł, danych wrażliwych lub finansowych. W przypadku informacji tajnych (haseł) zawsze preferowane jest kryptograficzne haszowanie i dodawanie ciągu inicjującego, a nie szyfrowanie haseł. Preferowane jest stosowanie metod uwierzytelniania, które eliminują konieczność przetwarzania haseł po stronie serwera;
- aktualizowanie systemu (oprogramowania komputerowego i oprogramowania układowego). Zapewnienie wszystkich środków bezpieczeństwa informatycznego, upewnienie się, że są one skuteczne oraz ich regularne aktualizowanie w przypadku zmiany lub rozwoju procesów lub okoliczności. Aby móc wykazać zgodność z art. 5 ust. 1 lit. f) zgodnie z art. 5 ust. 2 RODO, administrator powinien prowadzić rejestr wszystkich przeprowadzonych aktualizacji, w tym również czasu, w którym zostały one zastosowane;
- stosowanie silnych metod uwierzytelniania, takich jak uwierzytelnianie dwuskładnikowe i serwery uwierzytelniania, uzupełnionych aktualną polityką haseł;
- standardy bezpiecznego rozwoju obejmują filtrowanie danych wprowadzanych przez użytkownika (w miarę możliwości z wykorzystaniem białych list), anulowanie danych wprowadzanych przez użytkownika

[23] Więcej informacji na temat bezpiecznego tworzenia aplikacji internetowych można znaleźć także na stronie internetowej: https://www.owasp.org/index.php/Main_Page .

oraz środki zapobiegania atakom siłowym (takie jak ograniczanie maksymalnej liczby ponownych prób). W skutecznym stosowaniu tej techniki mogą pomóc „zapory aplikacji internetowej";
- wdrożenie rygorystycznej polityki zarządzania uprawnieniami użytkowników i kontrolą dostępu;
- stosowanie odpowiedniej, aktualnej, skutecznej i zintegrowanej zapory sieciowej, systemu wykrywania włamań oraz innych systemów ochrony obwodowej;
- systematyczne audyty bezpieczeństwa informatycznego i ocena luk w zabezpieczeniach (testy penetracyjne);
- regularne przeglądy i testowanie w celu zagwarantowania, że kopie zapasowe mogą być wykorzystane do przywrócenia danych, których integralność lub dostępność została naruszona;
- brak identyfikatora sesji w adresie URL w postaci zwykłego tekstu.

4 WEWNĘTRZNE ŹRÓDŁO RYZYKA LUDZKIEGO

71. Należy zwrócić uwagę na rolę błędu ludzkiego w naruszeniach ochrony danych osobowych ze względu na jego powszechne występowanie. Ponieważ tego typu naruszenia mogą być zarówno celowe, jak i niezamierzone, administratorom danych bardzo trudno jest zidentyfikować luki w zabezpieczeniach i przyjąć środki pozwalające ich uniknąć. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności uznała znaczenie zajęcia się takimi czynnikami ludzkimi i w październiku 2019 r. przyjęła rezolucję dotyczącą roli błędu ludzkiego w naruszeniach ochrony danych osobowych[24]. W rezolucji tej podkreślono, że należy zastosować odpowiednie środki zabezpieczające w celu zapobiegania błędom ludzkim, oraz przedstawiono niewyczerpujący wykaz takich zabezpieczeń i podejść.

4.1 PRZYPADEK nr 08: Eksfiltracja danych biznesowych przez pracownika

W okresie wypowiedzenia pracownik przedsiębiorstwa kopiuje dane biznesowe z bazy danych przedsiębiorstwa. Pracownik jest upoważniony do korzystania z tych danych wyłącznie w celu realizacji swoich zadań służbowych. Kilka miesięcy później, po odejściu z pracy, wykorzystuje uzyskane wówczas dane (podstawowe dane kontaktowe) do zasilenia nowego procesu przetwarzania danych, którego jest administratorem, w celu skontaktowania się z klientami przedsiębiorstwa, aby przyciągnąć ich do swojej nowej działalności.

4.1.1 PRZYPADEK nr 08 – Środki zapobiegawcze i ocena ryzyka

72. W tym konkretnym przypadku nie wprowadzono żadnych środków zapobiegających kopiowaniu przez pracownika danych kontaktowych klientów przedsiębiorstwa, ponieważ potrzebował on – i miał – uzasadniony dostęp do tych informacji w związku z wykonywanymi przez siebie zadaniami służbowymi. W związku z tym, że wykonywanie większości zadań związanych z relacjami z klientami wymaga od pracownika pewnego rodzaju dostępu do danych osobowych, takie naruszenia ochrony danych mogą być najtrudniejsze do zapobieżenia. Ograniczenia zakresu dostępu mogą ograniczyć pracę, którą dany pracownik jest w stanie wykonać. Jednak dobrze przemyślane zasady dostępu i stała kontrola mogą pomóc w zapobieganiu takim naruszeniom.

73. Jak zwykle, podczas oceny ryzyka należy wziąć pod uwagę rodzaj naruszenia oraz charakter, wrażliwość i ilość danych osobowych, których dotyczy naruszenie. Tego rodzaju naruszenia są zazwyczaj naruszeniami dotyczącymi poufności, ponieważ baza danych pozostaje zwykle nienaruszona, a jej zawartość jest „tylko"

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

kopiowana do dalszego wykorzystania. Ilość naruszonych danych jest zwykle niska lub średnia. W tym konkretnym przypadku nie naruszono żadnych szczególnych kategorii danych osobowych – pracownik potrzebował jedynie danych kontaktowych klientów, aby móc się z nimi skontaktować po odejściu z przedsiębiorstwa. Dlatego dane te nie są wrażliwe.

74. Chociaż jedyny cel byłego pracownika, który w złej wierze skopiował dane, może ograniczać się do zdobycia informacji kontaktowych o klientach przedsiębiorstwa do własnych celów handlowych, administrator nie może uznać ryzyka dla osób, których dane dotyczą, za niskie, ponieważ nie ma żadnej pewności co do intencji pracownika. Tak więc, choć konsekwencje naruszenia mogą być ograniczone do narażenia na niedopuszczalny marketing własny byłego pracownika, nie można wykluczyć dalszych i poważniejszych nadużyć skradzionych danych, w zależności od celu przetwarzania wprowadzonego przez byłego pracownika[25].

4.1.2 PRZYPADEK nr 08 – Łagodzenie skutków i obowiązki

75. Złagodzenie negatywnych skutków naruszenia w powyższym przypadku jest trudne. Konieczne może być podjęcie natychmiastowych działań prawnych, aby zapobiec dalszemu nadużywaniu i rozpowszechnianiu danych przez byłego pracownika. Kolejnym krokiem powinno być unikanie podobnych sytuacji w przyszłości. Administrator może próbować nakazać byłemu pracownikowi zaprzestanie wykorzystywania danych, ale powodzenie takiego działania jest w najlepszym wypadku wątpliwe. Pomocne mogą być odpowiednie środki techniczne, takie jak uniemożliwienie kopiowania lub pobierania danych na urządzenia wymienne.

76. Nie ma uniwersalnego rozwiązania dla tego typu przypadków, ale systematyczne podejście może pomóc w ich zapobieganiu. Na przykład przedsiębiorstwo może rozważyć – jeśli to możliwe – odebranie pewnych form dostępu pracownikom, którzy zasygnalizowali zamiar odejścia z pracy, lub wprowadzenie dzienników dostępu, tak aby niepożądany dostęp mógł być rejestrowany i oznaczany. Umowa podpisywana z pracownikami powinna zawierać klauzule zabraniające takich działań.

77. W sumie, ponieważ dane naruszenie nie spowoduje wysokiego ryzyka naruszenia praw i wolności osób fizycznych, wystarczy zgłoszenie organowi nadzorczemu. Zawiadomienie osób, których dane dotyczą, może być jednak korzystne również dla administratora, ponieważ lepiej, by dowiedziały się one o wycieku danych od przedsiębiorstwa, a nie od byłego pracownika, który próbuje się z nimi skontaktować. Dokumentacja naruszenia ochrony danych zgodnie z art. 33 ust. 5 jest obowiązkiem prawnym.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	X

[25] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

4.2 PRZYPADEK nr 09: Przypadkowe przesłanie danych do zaufanej strony trzeciej

Agent ubezpieczeniowy zauważył, że – przez błędne ustawienia pliku Excel otrzymanego pocztą elektroniczną – uzyskał dostęp do informacji dotyczących dwóch tuzinów klientów nienależących do jego zakresu obowiązków. Jest on zobowiązany do zachowania tajemnicy zawodowej i był jedynym odbiorcą wiadomości e-mail. Umowa pomiędzy administratorem danych a agentem ubezpieczeniowym zobowiązuje agenta do niezwłocznego sygnalizowania administratorowi danych naruszenia ochrony danych osobowych. Dlatego agent natychmiast zasygnalizował błąd administratorowi danych, który poprawił plik i wysłał go ponownie, prosząc agenta o usunięcie poprzedniej wiadomości. Zgodnie z powyższymi ustaleniami agent musi potwierdzić usunięcie danych w pisemnym oświadczeniu, co też uczynił. Uzyskane informacje nie zawierają żadnych szczególnych kategorii danych osobowych, a jedynie dane kontaktowe i dane dotyczące samego ubezpieczenia (rodzaj ubezpieczenia, kwota ubezpieczenia). Po przeanalizowaniu danych osobowych, których dotyczyło naruszenie, administrator nie stwierdził żadnych szczególnych cech po stronie osób lub administratora danych, które mogłyby wpłynąć na poziom skutków naruszenia.

4.2.1 PRZYPADEK nr 09 – Środki zapobiegawcze i ocena ryzyka

78. W tym przypadku naruszenie nie wynika z celowego działania pracownika, ale z niezamierzonego błędu ludzkiego spowodowanego nieuwagą. Tego rodzaju naruszeń można uniknąć lub zmniejszyć ich częstotliwość poprzez: a) wprowadzenie programów szkoleniowych, edukacyjnych i uświadamiających, w ramach których pracownicy lepiej rozumieją znaczenie ochrony danych osobowych, b) ograniczenie wymiany plików za pośrednictwem poczty elektronicznej, a zamiast tego korzystanie z dedykowanych systemów służących np. do przetwarzania danych klientów, c) podwójne sprawdzanie plików przed ich wysłaniem, d) rozdzielenie procesu tworzenia i wysyłania plików.

79. To naruszenie ochrony danych dotyczy tylko poufności danych, a ich integralność i dostępność pozostają nienaruszone. Naruszenie ochrony danych dotyczyło jedynie około dwóch tuzinów klientów, dlatego ilość naruszonych danych można uznać za niewielką. Ponadto dane osobowe, których dotyczyło naruszenie, nie zawierały żadnych danych wrażliwych. Fakt, że podmiot przetwarzający dane natychmiast skontaktował się z administratorem danych po uzyskaniu informacji o naruszeniu ochrony danych, można uznać za czynnik ograniczający ryzyko. (Należy również ocenić możliwość przesłania danych do innych agentów ubezpieczeniowych, a w razie potwierdzenia należy zastosować odpowiednie środki). Ze względu na odpowiednie kroki podjęte po naruszeniu ochrony danych, prawdopodobnie nie będzie ono miało żadnego wpływu na prawa i wolności osób, których dane dotyczą.

80. Połączenie niewielkiej liczby osób, których dotyczy naruszenie, natychmiastowego wykrycia naruszenia oraz środków podjętych w celu zminimalizowania jego skutków sprawia, że ten przypadek nie stanowi zagrożenia.

4.2.2 PRZYPADEK nr 09 – Łagodzenie skutków i obowiązki

81. Ponadto w grę wchodzą również inne okoliczności zmniejszające ryzyko: agent jest zobowiązany do zachowania tajemnicy zawodowej, sam zgłosił problem administratorowi i usunął plik na żądanie. Podniesienie świadomości i ewentualne uwzględnienie dodatkowych kroków przy sprawdzaniu dokumentów zawierających dane osobowe prawdopodobnie pomoże uniknąć podobnych przypadków w przyszłości.

82. Poza udokumentowaniem naruszenia zgodnie z art. 33 ust. 5 nie ma potrzeby podejmowania żadnych innych działań.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	X	X

4.3 Środki organizacyjne i techniczne służące zapobieganiu skutkom wewnętrznych źródeł ryzyka ludzkiego i ich łagodzeniu

83. **Połączenie wymienionych poniżej środków – stosowanych w zależności od specyfiki danego przypadku – powinno pomóc zmniejszyć prawdopodobieństwo ponownego wystąpienia podobnego naruszenia.**

84. Zalecane środki:

(*Lista poniższych środków nie jest w żadnym wypadku wyłączna ani wyczerpująca. Celem jest raczej przedstawienie pomysłów na zapobieganie atakom i możliwych rozwiązań. Każda czynność przetwarzania danych jest inna, dlatego administrator powinien podjąć decyzję, które środki najbardziej pasują do danej sytuacji*.)

- okresowe wdrażanie programów szkoleniowych, edukacyjnych i poszerzających wiedzę dla pracowników w zakresie ich obowiązków dotyczących prywatności i bezpieczeństwa oraz wykrywania i zgłaszania zagrożeń dla bezpieczeństwa danych osobowych[26]. Opracowanie programu poszerzającego wiedzę pracowników w zakresie najczęstszych błędów prowadzących do naruszenia ochrony danych osobowych i sposobów ich unikania;
- ustanowienie solidnych i skutecznych praktyk, procedur i systemów w zakresie ochrony danych i prywatności[27];
- ocena praktyk, procedur i systemów ochrony prywatności w celu zapewnienia ich ciągłej skuteczności[28];
- tworzenie odpowiednich zasad kontroli dostępu i wymaganie od użytkowników przestrzegania tych zasad;
- wdrażanie technik wymuszania uwierzytelniania użytkownika w przypadku dostępu do wrażliwych danych osobowych;
- wyłączenie konta służbowego użytkownika, gdy tylko odejdzie on z przedsiębiorstwa;
- sprawdzanie nietypowych przepływów danych między serwerem plików a stacjami roboczymi pracowników;
- ustawienie zabezpieczeń interfejsów wejścia/wyjścia w systemie BIOS lub za pomocą oprogramowania kontrolującego korzystanie z interfejsów komputerowych (blokowanie lub odblokowywanie np. USB/CD/DVD itp.);
- weryfikacja polityki dostępu pracowników (np. rejestrowanie dostępu do danych wrażliwych i wymaganie od użytkownika podania powodu biznesowego, tak aby było to dostępne podczas audytu);
- wyłączenie otwartych usług w chmurze;
- zakazanie i uniemożliwienie dostępu do znanych otwartych usług pocztowych;
- wyłączenie funkcji „print screen” w systemie operacyjnym;
- egzekwowanie polityki czystego biurka;
- automatyczne blokowanie wszystkich komputerów po określonym czasie bezczynności;

---

[26] Sekcja 2) pkt (i) rezolucji dotyczącej roli błędu ludzkiego w naruszeniach ochrony danych osobowych.

[27] Sekcja 2) pkt (ii) rezolucji dotyczącej roli błędu ludzkiego w naruszeniach ochrony danych osobowych.

[28] Sekcja 2) pkt (iii) rezolucji dotyczącej roli błędu ludzkiego w naruszeniach ochrony danych osobowych.

- wykorzystanie mechanizmów (np. (bezprzewodowego) tokena do logowania/otwierania zablokowanych kont) do szybkiego przełączania użytkowników w środowiskach współdzielonych;
- wykorzystanie specjalnych systemów do zarządzania danymi osobowymi, które stosują odpowiednie mechanizmy kontroli dostępu i zapobiegają błędom ludzkim, takim jak wysyłanie wiadomości do niewłaściwych osób. Korzystanie z arkuszy kalkulacyjnych i innych dokumentów biurowych nie jest właściwym sposobem zarządzania danymi klientów.

5 ZAGUBIONE LUB SKRADZIONE URZĄDZENIA I DOKUMENTY PAPIEROWE

85. Częstym przypadkiem jest utrata lub kradzież urządzeń przenośnych. W takich przypadkach administrator musi wziąć pod uwagę okoliczności operacji przetwarzania, takie jak rodzaj danych przechowywanych na urządzeniu, a także aktywa pomocnicze oraz środki podjęte przed naruszeniem w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Wszystkie te elementy mają wpływ na potencjalne skutki naruszenia ochrony danych. Ocena ryzyka może być trudna, ponieważ urządzenie nie jest już dostępne.

86. Tego rodzaju naruszenia zawsze można zaklasyfikować jako naruszenia dotyczące poufności. Jeżeli jednak nie istnieje kopia zapasowa skradzionej bazy danych, może to być również naruszenie dotyczące dostępności i integralności.

87. Poniższe scenariusze pokazują, w jaki sposób wyżej wymienione okoliczności wpływają na prawdopodobieństwo i dotkliwość naruszenia ochrony danych.

5.1 PRZYPADEK nr 10: Skradziony materiał przechowujący zaszyfrowane dane osobowe

Podczas włamania do świetlicy środowiskowej skradziono dwa tablety. Na tabletach znajdowała się aplikacja, która zawierała dane osobowe dzieci uczęszczających do świetlicy. Dotyczyło to imion i nazwisk, dat urodzenia, danych osobowych związanych z edukacją dzieci. Zarówno zaszyfrowane tablety, które w momencie włamania były wyłączone, jak i aplikacja były chronione silnym hasłem. Dane zapasowe były skutecznie i łatwo dostępne dla administratora. Po uzyskaniu informacji o włamaniu opiekun świetlicy wydał zdalne polecenie wyczyszczenia tabletów wkrótce po odkryciu włamania.

5.1.1 PRZYPADEK nr 10 – Środki zapobiegawcze i ocena ryzyka

88. W tym konkretnym przypadku administrator danych zastosował odpowiednie środki, by zapobiec potencjalnemu naruszeniu ochrony danych i złagodzić jego skutki, stosując szyfrowanie urządzeń, wprowadzając odpowiednią ochronę hasłem i zabezpieczając kopie zapasowe danych przechowywanych na tabletach. (Wykaz zalecanych środków można znaleźć w sekcji 5.7).

89. Po uzyskaniu informacji o naruszeniu administrator powinien ocenić źródło ryzyka, systemy wspierające przetwarzanie danych, rodzaj danych osobowych, których dotyczy naruszenie, oraz potencjalny wpływ naruszenia ochrony danych na osoby, których ono dotyczy. Opisane powyżej naruszenie ochrony danych dotyczyłoby poufności, dostępności i integralności danych, jednak dzięki odpowiedniemu postępowaniu administratora danych przed i po naruszeniu ochrony danych nie doszło do żadnego z tych przypadków.

5.1.2 PRZYPADEK nr 10 – Łagodzenie skutków i obowiązki

90. Poufność danych osobowych znajdujących się na urządzeniach nie została naruszona dzięki silnej ochronie hasłem zarówno tabletów, jak i aplikacji. Tablety skonfigurowano w taki sposób, że ustawienie hasła oznacza również, że dane na urządzeniu są szyfrowane. Zostało to dodatkowo wzmocnione przez działania administratora polegające na próbie zdalnego wyczyszczenia wszystkich danych ze skradzionych urządzeń.

91. Dzięki podjętym środkom poufność danych również pozostała nienaruszona. Ponadto kopie zapasowe zapewniały ciągłą dostępność danych osobowych, a zatem nie mogły wystąpić żadne potencjalne negatywne skutki.

92. W związku z powyższym opisane powyżej naruszenie ochrony danych prawdopodobnie nie spowodowało ryzyka naruszenia praw i wolności osób, których dane dotyczą, dlatego też nie było konieczności powiadamiania organu nadzorczego ani osób, których dane dotyczą. Takie naruszenie ochrony danych musi być jednak udokumentowane zgodnie z art. 33 ust. 5.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	X	X

5.2 PRZYPADEK nr 11: Skradziony materiał przechowujący niezaszyfrowane dane osobowe

Skradziono elektroniczny notebook pracownika przedsiębiorstwa świadczącego usługi. Skradziony notebook zawierał imiona, nazwiska, płeć, adresy i daty urodzenia ponad 100 000 klientów. Ze względu na niedostępność skradzionego urządzenia nie można było ustalić, czy naruszona została ochrona także innych kategorii danych osobowych. Dostęp do dysku twardego notebooka nie był chroniony żadnym hasłem. Dane osobowe można było przywrócić z dostępnych codziennych kopii zapasowych.

5.2.1 PRZYPADEK nr 11 – Środki zapobiegawcze i ocena ryzyka

93. Administrator nie wprowadził żadnych wcześniejszych środków bezpieczeństwa, dlatego też dane osobowe przechowywane na skradzionym notebooku były łatwo dostępne dla złodzieja lub każdej innej osoby, która weszła w posiadanie tego urządzenia w późniejszym czasie.

94. To naruszenie ochrony danych dotyczy poufności danych przechowywanych na skradzionym urządzeniu.

95. Notebook zawierający dane osobowe był w tym przypadku podatny na ataki, ponieważ nie był chroniony hasłem ani szyfrowaniem. Brak podstawowych środków bezpieczeństwa zwiększa poziom ryzyka w przypadku osób, których dane dotyczą. Ponadto identyfikacja osób, których dane dotyczą, jest także problematyczna, co dodatkowo zwiększa stopień szkodliwości naruszenia. Znaczna liczba osób, których dane dotyczą, zwiększa ryzyko, niemniej jednak naruszenie ochrony danych nie dotyczyło żadnych szczególnych kategorii danych osobowych.

96. Podczas oceny ryzyka[29] administrator powinien wziąć pod uwagę potencjalne konsekwencje i negatywne skutki naruszenia dotyczącego poufności. W wyniku naruszenia osoby, których dane dotyczą, mogą paść ofiarą oszustwa dotyczącego tożsamości w związku z danymi dostępnymi na skradzionym urządzeniu, dlatego ryzyko uznaje się za wysokie.

[29] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

5.2.2 PRZYPADEK nr 11 – Łagodzenie skutków i obowiązki

97. Włączenie szyfrowania urządzeń i zabezpieczenie przechowywanej bazy danych silnym hasłem mogło zapobiec naruszeniu danych, które mogłoby spowodować ryzyko naruszenia praw i wolności osób, których dane dotyczą.

98. W związku z tymi okolicznościami wymagane jest zgłoszenie naruszenia organowi nadzorczemu, a także zawiadomienie osób, których dane dotyczą.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	✓

5.3 PRZYPADEK nr 12: Skradzione dokumenty w formie papierowej z danymi wrażliwymi

Z ośrodka odwykowego skradziono papierowy rejestr. Rejestr zawierał podstawowe dane identyfikacyjne i zdrowotne pacjentów przyjętych do ośrodka odwykowego. Dane były przechowywane tylko w wersji papierowej, a lekarze leczący pacjentów nie mieli dostępu do kopii zapasowych. Rejestru nie przechowywano w zamkniętej szufladzie ani zamkniętym pomieszczeniu, administrator danych nie stosował systemu kontroli dostępu ani żadnych innych środków zabezpieczających dokumentację papierową.

5.3.1 PRZYPADEK nr 12 – Środki zapobiegawcze i ocena ryzyka

99. Administrator nie wprowadził żadnych wcześniejszych środków bezpieczeństwa, dlatego też dane osobowe przechowywane w tym rejestrze były łatwo dostępne dla osoby, która go znalazła. Ponadto ze względu na charakter danych osobowych przechowywanych w rejestrze brak kopii zapasowej stanowi bardzo poważny czynnik ryzyka.

100. Ten przypadek stanowi przykład naruszenia ochrony danych o wysokim ryzyku. Ze względu na brak odpowiednich środków ostrożności utracono dane, które zgodnie z art. 9 ust. 1 RODO stanowią wrażliwe dane dotyczące zdrowia. Ponieważ w tym przypadku chodziło o szczególną kategorię danych osobowych, potencjalne ryzyko dla osób, których dane dotyczą, było zwiększone, co powinien również wziąć pod uwagę administrator oceniający ryzyko[30].

101. Naruszenie to dotyczy poufności, dostępności i integralności danych osobowych. W wyniku naruszenia naruszona zostaje tajemnica lekarska, a nieuprawnione osoby trzecie mogą uzyskać dostęp do prywatnych informacji medycznych pacjentów, co może mieć poważny wpływ na życie osobiste pacjenta. Naruszenie dotyczące dostępności danych może również zakłócić ciągłość leczenia pacjentów. W związku z tym, że nie można wykluczyć modyfikacji/usunięcia części zawartości rejestru, zagrożona jest także integralność danych osobowych.

5.3.2 PRZYPADEK nr 12 – Łagodzenie skutków i obowiązki

102. Podczas oceny środków zabezpieczających należy również wziąć pod uwagę rodzaj aktywów pomocniczych. W związku z tym, że rejestr pacjentów była dokumentem fizycznym, jego zabezpieczenie powinno być zorganizowane inaczej niż w przypadku urządzenia elektronicznego. Pseudonimizacja nazwisk pacjentów, przechowywanie rejestru w zabezpieczonych pomieszczeniach, w zamkniętej szufladzie lub pokoju oraz

[30] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

właściwa kontrola dostępu z uwierzytelnianiem podczas uzyskiwania dostępu do rejestru mogły zapobiec naruszeniu ochrony danych.

103. Opisane powyżej naruszenie ochrony danych może mieć poważne skutki dla osób, których dane dotyczą; dlatego też zgłoszenie organowi nadzorczemu i zawiadomienie o naruszeniu osób, których dane dotyczą, jest obowiązkowe.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	✓

5.4 Środki organizacyjne i techniczne służące zapobieganiu skutkom utraty lub kradzieży urządzeń i ich łagodzeniu

104. Połączenie wymienionych poniżej środków – stosowanych w zależności od specyfiki danego przypadku – powinno pomóc zmniejszyć prawdopodobieństwo ponownego wystąpienia podobnego naruszenia.

105. Zalecane środki:

(*Lista poniższych środków nie jest w żadnym wypadku wyłączna ani wyczerpująca. Celem jest raczej przedstawienie pomysłów na zapobieganie atakom i możliwych rozwiązań. Każda czynność przetwarzania danych jest inna, dlatego administrator powinien podjąć decyzję, które środki najbardziej pasują do danej sytuacji.*)

- włączenie szyfrowania urządzenia (takiego jak Bitlocker, Veracrypt lub DM-Crypt);
- używanie kodu/hasła na wszystkich urządzeniach. Szyfrowanie wszystkich przenośnych urządzeń elektronicznych w sposób, który wymaga wprowadzenia złożonego hasła w celu ich odszyfrowania;
- stosowanie uwierzytelniania wieloskładnikowego;
- włączenie w urządzeniach mobilnych funkcji umożliwiających ich lokalizację w przypadku utraty lub zgubienia;
- stosowanie oprogramowania/aplikacji MDM (zarządzanie urządzeniami mobilnymi) i lokalizacji. Stosowanie filtrów antyodblaskowych. Wyłączanie wszelkich urządzeń pozostawionych bez nadzoru;
- jeżeli to możliwe i właściwe dla danego przetwarzania danych – zapisanie danych osobowych nie na urządzeniu mobilnym, ale na centralnym serwerze wewnętrznym;
- jeżeli stacja robocza jest podłączona do firmowej sieci LAN – wykonanie automatycznej kopii zapasowej z folderów roboczych, o ile nie da się uniknąć przechowywania w nich danych osobowych;
- używanie bezpiecznej sieci VPN (np. takiej, która wymaga osobnego klucza uwierzytelniania drugiego składnika w celu ustanowienia bezpiecznego połączenia) do łączenia urządzeń mobilnych z serwerami wewnętrznymi;
- udostępnienie pracownikom fizycznych blokad, aby umożliwić im fizyczne zabezpieczenie urządzeń mobilnych, z których korzystają, gdy pozostają one bez nadzoru;
- właściwe uregulowanie kwestii korzystania z urządzeń poza przedsiębiorstwem;
- właściwe uregulowanie kwestii korzystania z urządzeń wewnątrz przedsiębiorstwa;
- stosowanie oprogramowania/aplikacji MDM (zarządzanie urządzeniami mobilnymi) i włączenie funkcji zdalnego czyszczenia danych;
- stosowanie scentralizowanego zarządzania urządzeniami z minimalnymi uprawnieniami użytkowników końcowych do instalowania oprogramowania;
- zainstalowanie fizycznej kontroli dostępu;
- unikanie przechowywania informacji szczególnie chronionych na urządzeniach mobilnych i na dyskach twardych. Jeżeli istnieje potrzeba dostępu do wewnętrznego systemu przedsiębiorstwa, należy korzystać z bezpiecznych kanałów, takich jak opisane wcześniej.

6 BŁĘDNE PRZESŁANIE WIADOMOŚCI

106. Również w tym przypadku źródłem ryzyka jest wewnętrzny błąd ludzki, ale w tym przypadku do naruszenia nie doprowadziło żadne złośliwe działanie. Jest ono wynikiem nieuwagi. Po jego wystąpieniu administrator niewiele może zrobić, dlatego w takich przypadkach zapobieganie jest jeszcze ważniejsze niż w przypadku innych rodzajów naruszeń.

6.1 PRZYPADEK nr 13: Pomyłka pocztowa

Przedsiębiorstwo zajmujące się sprzedażą detaliczną zapakowała dwa zamówienia na buty. Z powodu błędu ludzkiego pomylono dwa listy przewozowe, w wyniku czego oba produkty i odpowiednie listy przewozowe zostały wysłane do niewłaściwych osób. Oznacza to, że obaj klienci otrzymali wzajemnie swoje zamówienia, w tym listy przewozowe zawierające dane osobowe. Po uzyskaniu informacji o naruszeniu administrator danych wycofał zamówienia i wysłał je do właściwych odbiorców.

6.1.1 PRZYPADEK nr 13 – Środki zapobiegawcze i ocena ryzyka

107. Listy przewozowe zawierały dane osobowe wymagane do skutecznej dostawy (imię i nazwisko, adres oraz zakupiony towar i jego cenę). Ważne jest ustalenie, jak w ogóle mogło dojść do błędu ludzkiego i czy w jakikolwiek sposób można było mu zapobiec. W opisywanym przypadku ryzyko jest niskie, ponieważ nie dotyczy szczególnych kategorii danych osobowych ani innych danych, których nadużycie mogłoby mieć istotne negatywne skutki, naruszenie nie jest wynikiem systemowego błędu po stronie administratora i dotyczy tylko dwóch osób. Nie można zidentyfikować żadnych negatywnych skutków dla tych osób.

6.1.2 PRZYPADEK nr 13 – Łagodzenie skutków i obowiązki

108. Administrator powinien zapewnić bezpłatny zwrot przedmiotów i dołączonych do nich listów przewozowych, a także zwrócić się do niewłaściwych odbiorców o zniszczenie/usunięcie wszystkich ewentualnych kopii listów przewozowych zawierających dane osobowe drugiej osoby.

109. Nawet jeśli samo naruszenie nie stwarza wysokiego ryzyka dla praw i wolności osób, których dane dotyczą, a zatem przekazywanie informacji osobom, których dane dotyczą, nie jest wymagane na mocy art. 34 RODO, nie można unikać zawiadomienia tych osób o naruszeniu, ponieważ ich współpraca jest niezbędna do ograniczenia ryzyka.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	X	X

6.2 PRZYPADEK nr 14: Omyłkowe wysłanie pocztą wysoce poufnych danych osobowych

Dział zatrudnienia urzędu administracji publicznej wysłał wiadomość e-mail – o zbliżających się szkoleniach – do osób zarejestrowanych w jego systemie jako poszukujące pracy. Przez pomyłkę do wiadomości e-mail dołączono dokument zawierający dane osobowe wszystkich osób poszukujących pracy (imię i nazwisko, adres e-mail, adres pocztowy, numer ubezpieczenia społecznego). Liczba osób, których to dotyczy, wynosi ponad 60 000. Następnie urząd skontaktował się ze wszystkimi odbiorcami i poprosił ich o usunięcie poprzedniej wiadomości oraz o niewykorzystywanie zawartych w niej informacji.

6.2.1 PRZYPADEK nr 14 – Środki zapobiegawcze i ocena ryzyka

110. Należało wprowadzić bardziej rygorystyczne zasady wysyłania takich wiadomości. Należy rozważyć wprowadzenie dodatkowych mechanizmów kontroli.

111. Liczba osób, których dotyczy naruszenie, jest znaczna, a wykorzystanie numeru ubezpieczenia społecznego oraz innych, bardziej podstawowych danych osobowych dodatkowo zwiększa ryzyko, które można określić jako wysokie[31]. Administrator nie jest w stanie zapobiec ewentualnemu rozpowszechnianiu danych przez któregokolwiek z odbiorców.

6.2.2 PRZYPADEK nr 14 – Łagodzenie skutków i obowiązki

112. Jak wspomniano wcześniej, środki skutecznego ograniczania ryzyka podobnego naruszenia są ograniczone. Mimo że administrator poprosił odbiorców o usunięcie wiadomości, nie może ich zmusić do tego, a w konsekwencji nie może być pewien, że zastosują się oni do tego żądania.

113. Wykonanie wszystkich trzech wskazanych poniżej czynności powinno być oczywiste w przypadku takim jak ten.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	✓

6.3 PRZYPADEK nr 15: Omyłkowe wysłanie pocztą danych osobowych

Lista uczestników kursu prawniczego języka angielskiego, który odbywa się w hotelu przez 5 dni, została przez pomyłkę wysłana do 15 byłych uczestników kursu zamiast do hotelu. Lista zawiera imiona i nazwiska, adresy e-mail i preferencje żywieniowe 15 uczestników. Tylko dwóch uczestników wypełniło formularz dotyczący preferencji żywieniowych, informując, że nie tolerują laktozy. Żaden z uczestników nie ma chronionej tożsamości. Administrator odkrył błąd natychmiast po wysłaniu listy i poinformował o nim odbiorców, prosząc ich o usunięcie listy.

6.3.1 PRZYPADEK nr 15 – Środki zapobiegawcze i ocena ryzyka

114. Należało wdrożyć rygorystyczne zasady wysyłania wiadomości zawierających dane osobowe. Należy rozważyć wprowadzenie dodatkowych mechanizmów kontroli.

115. Ryzyko wynikające z charakteru, wrażliwości, ilości i kontekstu danych osobowych jest niskie. Dane osobowe obejmują dane wrażliwe dotyczące preferencji żywieniowych dwóch uczestników. Nawet jeśli informacja o tym, że ktoś nie toleruje laktozy, stanowi dane dotyczące zdrowia, ryzyko, że dane te zostaną wykorzystane w szkodliwy sposób, należy uznać za stosunkowo niskie. Chociaż w przypadku danych dotyczących zdrowia zwykle zakłada się, że naruszenie może spowodować wysokie ryzyko dla osoby, której dane dotyczą[32], to jednocześnie w tym konkretnym przypadku nie można zidentyfikować ryzyka, że naruszenie doprowadzi do fizycznej, materialnej lub niematerialnej szkody osoby, której dane dotyczą, z powodu nieuprawnionego ujawnienia informacji o nietolerancji laktozy. W przeciwieństwie do niektórych innych preferencji żywieniowych, nietolerancji laktozy zwykle nie można powiązać z żadnymi przekonaniami religijnymi lub

[31] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

[32] Zob. Wytyczne WP 250, s. 23.

filozoficznymi. Ilość naruszonych danych i liczba poszkodowanych osób, których dane dotyczą, jest również bardzo niska.

6.3.2 PRZYPADEK nr 15 – Łagodzenie skutków i obowiązki

116. Podsumowując, można stwierdzić, że naruszenie nie miało znaczącego wpływu na osoby, których dane dotyczą. Za okoliczność łagodzącą można uznać fakt, że administrator danych niezwłocznie skontaktował się z odbiorcami po uzyskaniu informacji o błędzie.

117. Jeżeli wiadomość e-mail została wysłana do niewłaściwego/nieuprawnionego odbiorcy, zaleca się, aby administrator danych przesłał wiadomość UDW do niezamierzonych odbiorców z przeprosinami, poleceniem usunięcia wiadomości e-mail stanowiącej naruszenie oraz informacją, że odbiorcy nie mają prawa do dalszego korzystania ze wskazanych im adresów e-mail.

118. W związku z powyższym naruszenie ochrony danych prawdopodobnie nie spowodowało ryzyka naruszenia praw i wolności osób, których dane dotyczą, dlatego też nie było konieczności powiadamiania organu nadzorczego ani osób, których dane dotyczą. Takie naruszenie ochrony danych musi być jednak udokumentowane zgodnie z art. 33 ust. 5.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	X	X

6.4 PRZYPADEK nr 16: Pomyłka pocztowa

Grupa ubezpieczeniowa oferuje ubezpieczenia samochodowe. W tym celu regularnie wysyła pocztą dostosowywane polisy składkowe. Oprócz imienia i nazwiska oraz adresu posiadacza polisy, list zawiera numer rejestracyjny pojazdu bez zamazanych cyfr, stawki ubezpieczeniowe na bieżący i następny rok ubezpieczeniowy, przybliżony roczny przebieg oraz datę urodzenia posiadacza polisy. Nie zawiera natomiast danych dotyczących zdrowia zgodnie z art. 9 RODO, danych dotyczących płatności (dane bankowe) oraz danych ekonomicznych i finansowych.

Listy są pakowane za pomocą automatycznych maszyn kopertujących. Z powodu błędu mechanicznego do jednej koperty włożono dwa listy dla różnych ubezpieczających i wysłano je do jednego ubezpieczającego pocztą listową. Ubezpieczający otworzył list w domu i zapoznał się ze swoim prawidłowo dostarczonym listem oraz z nieprawidłowo dostarczonym listem do innego ubezpieczającego.

6.4.1 PRZYPADEK nr 16 – Środki zapobiegawcze i ocena ryzyka

119. Nieprawidłowo doręczony list zawiera imię i nazwisko, adres, datę urodzenia, niezamazany numer rejestracyjny pojazdu oraz klasyfikację stawki ubezpieczeniowej w bieżącym i przyszłym roku. Skutki dla osoby poszkodowanej należy uznać za średnie, ponieważ informacje niedostępne publicznie, takie jak data urodzenia lub niezamazane numery rejestracyjne pojazdów, a także szczegóły dotyczące wzrostu stawek ubezpieczeniowych zostały ujawnione nieuprawnionemu odbiorcy. Prawdopodobieństwo niewłaściwego wykorzystania tych danych ocenia się na poziomie od niskiego do średniego. Choć wielu odbiorców prawdopodobnie wyrzuci błędnie otrzymany list do śmieci, w pojedynczych przypadkach nie można całkowicie wykluczyć, że list zostanie umieszczony w serwisach społecznościowych lub że skontaktuje się z nim właściciel polisy.

6.4.2 PRZYPADEK nr 16 – Łagodzenie skutków i obowiązki

120. Administrator powinien na własny koszt zlecić zwrot oryginału dokumentu. Należy również poinformować błędnego odbiorcę, że nie może on w sposób niewłaściwy wykorzystać przeczytanych informacji.

121. Prawdopodobnie nigdy nie będzie możliwe całkowite zapobieżenie błędowi doręczenia pocztowego w masowej korespondencji przy użyciu w pełni zautomatyzowanych maszyn. W przypadku zwiększonej częstotliwości należy jednak sprawdzić, czy maszyny kopertujące są wystarczająco dobrze ustawione i konserwowane lub czy do takiego naruszenia nie prowadzi jakiś inny problem systemowy.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	X

6.5 Środki organizacyjne i techniczne służące zapobieganiu skutkom błędnego przesłania wiadomości i ich łagodzeniu

122. Połączenie wymienionych poniżej środków – stosowanych w zależności od specyfiki danego przypadku – powinno pomóc zmniejszyć prawdopodobieństwo ponownego wystąpienia podobnego naruszenia.

123. Zalecane środki:

(*Lista poniższych środków nie jest w żadnym wypadku wyłączna ani wyczerpująca. Celem jest raczej przedstawienie pomysłów na zapobieganie atakom i możliwych rozwiązań. Każda czynność przetwarzania danych jest inna, dlatego administrator powinien podjąć decyzję, które środki najbardziej pasują do danej sytuacji*.)

- ustalenie dokładnych standardów – bez możliwości interpretacji – wysyłania listów / wiadomości e-mail;
- odpowiednie szkolenie personelu w zakresie wysyłania listów / wiadomości e-mail;
- w przypadku wysyłania wiadomości e-mail do wielu odbiorców są oni domyślnie wymieniani w polu „UDW”;
- w przypadku wysyłania wiadomości e-mail do wielu odbiorców wymagane jest dodatkowe potwierdzenie i nie są oni wymienieni w polu „UDW”;
- zastosowanie zasady „czworga oczu”;
- automatyczne adresowanie zamiast ręcznego, z danymi pobranymi z dostępnej i aktualnej bazy danych; system automatycznego adresowania powinien być regularnie poddawany przeglądowi w celu sprawdzenia, czy nie ma w nim ukrytych błędów i nieprawidłowych ustawień;
- stosowanie opóźnienia w wysyłaniu wiadomości (np. możliwość usunięcia/edytowania w określonym czasie po kliknięciu przycisku „wyślij”);
- wyłączenie autouzupełniania podczas wpisywania adresów e-mail;
- sesje poszerzające wiedzę na temat najczęstszych błędów prowadzących do naruszenia ochrony danych osobowych;
- szkolenia i instrukcje dotyczące postępowania w przypadku incydentów prowadzących do naruszenia ochrony danych osobowych oraz tego, kogo należy o tym poinformować (zaangażować inspektora ochrony danych).

7 INNE PRZYPADKI – INŻYNIERIA SPOŁECZNA

7.1 PRZYPADEK nr 17: Kradzież tożsamości

Centrum kontaktowe przedsiębiorstwa telekomunikacyjnego otrzymuje telefon od osoby podającej się za klienta. Domniemany klient żąda od przedsiębiorstwa zmiany adresu e-mail, na który od tej pory mają być przesyłane informacje o rozliczeniach. Pracownik centrum kontaktowego weryfikuje tożsamość klienta, prosząc o podanie pewnych danych osobowych, zgodnie z procedurami obowiązującymi w przedsiębiorstwie. Osoba dzwoniąca prawidłowo podaje numer identyfikacji podatkowej i adres pocztowy klienta (ponieważ miała dostęp do tych danych). Po zatwierdzeniu operator dokonuje żądanej zmiany i od tego momentu informacje rozliczeniowe są przesyłane na nowy adres e-mail. Procedura ta nie przewiduje żadnego powiadomienia poprzedniego kontaktu e-mailowego. W następnym miesiącu prawowity klient kontaktuje się z przedsiębiorstwem, pytając, dlaczego nie otrzymuje faktur na swój adres e-mail, i zaprzecza, jakoby dzwonił z żądaniem zmiany adresu e-mail. Później pracownik przedsiębiorstwa uświadamia sobie, że informacje wysłano do nieuprawnionego użytkownika i wycofuje zmianę.

7.1.1 PRZYPADEK nr 17 – Ocena ryzyka, łagodzenie skutków i zobowiązania

124. Przypadek ten stanowi przykład znaczenia środków zapobiegawczych. Z punktu widzenia ryzyka naruszenie wiąże się z wysokim poziomem zagrożenia33, ponieważ dane rozliczeniowe mogą dostarczać informacji o życiu prywatnym osoby, której dane dotyczą (np. nawyki, kontakty) i mogą prowadzić do szkód materialnych (np. uporczywe nękanie, zagrożenie integralności fizycznej). Dane osobowe uzyskane podczas tego ataku mogą być również wykorzystane w celu ułatwienia przejęcia konta w tej organizacji lub wykorzystania dalszych środków uwierzytelniania w innych organizacjach. Biorąc pod uwagę te zagrożenia, „odpowiedni" środek uwierzytelniania powinien spełniać wysokie wymagania, w zależności od tego, jakie dane osobowe mogą być przetwarzane w wyniku uwierzytelniania.

125. W związku z tym administrator danych musi dokonać zarówno zgłoszenia do organu nadzorczego, jak i zawiadomić o tym osobę, której dane dotyczą.

126. Wcześniejszy proces uwierzytelniania klienta wyraźnie wymaga dopracowania w świetle tej sprawy. Metody zastosowane do uwierzytelniania nie były wystarczające. Złośliwa strona trzecia była w stanie udawać docelowego użytkownika, wykorzystując publicznie dostępne informacje oraz informacje, do których zyskała dostęp w inny sposób.

127. Nie zaleca się stosowania tego typu statycznego uwierzytelniania opartego na wiedzy (gdy odpowiedź nie ulega zmianie, a informacje nie są „tajne", jak w przypadku hasła).

128. Zamiast tego organizacja powinna stosować taką formę uwierzytelniania, która daje wysoki stopień pewności, że uwierzytelniany użytkownik jest osobą docelową, a nie kimś innym. Wprowadzenie pozapasmowej metody uwierzytelniania wieloskładnikowego rozwiązałoby ten problem, np. w celu weryfikacji żądania zmiany, wysyłając prośbę o potwierdzenie do poprzedniego kontaktu; lub dodając dodatkowe pytania i wymagając informacji widocznych tylko na poprzednich rachunkach. Decyzja o tym,

[33] Szczegółowe informacje na temat operacji przetwarzania, które „mogą powodować wysokie ryzyko" można znaleźć w przypisie 10 powyżej.

jakie środki wprowadzić, należy do administratora danych, ponieważ to on najlepiej zna szczegóły i wymogi swojej wewnętrznej działalności.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	✓

7.2 PRZYPADEK nr 18: Eksfiltracja poczty elektronicznej

Sieć hipermarketów wykryła trzy miesiące po konfiguracji, że niektóre konta poczty elektronicznej zostały zmienione i stworzono reguły, zgodnie z którymi każda wiadomość e-mail zawierająca określone wyrażenia (np. „faktura", „płatność", „przelew bankowy", „uwierzytelnienie karty kredytowej", „dane rachunku bankowego") była przenoszona do nieużywanego folderu i przekazywana na zewnętrzny adres e-mail. Ponadto do tego czasu przeprowadzono już atak socjotechniczny, tzn. sprawca ataku, podając się za dostawcę, zmienił dane rachunku bankowego dostawcy na swoje własne. Ponadto wysłano już kilka fałszywych faktur zawierających nowe dane rachunku bankowego. System monitorujący platformy poczty elektronicznej wydał ostrzeżenie dotyczące folderów. Przedsiębiorstwo nie było w stanie wykryć, w jaki sposób sprawca ataku uzyskał dostęp do kont pocztowych, ale przypuszczało, że winę za udzielenie dostępu grupie użytkowników odpowiedzialnych za płatności ponosiła zainfekowana wiadomość e-mail.

Dzięki przekazywaniu wiadomości e-mail opartych na słowach kluczowych atakujący uzyskał informacje o 99 pracownikach: imię i nazwisko oraz wynagrodzenie w danym miesiącu w odniesieniu do 89 osób, których dane dotyczą; imię i nazwisko, stan cywilny, liczba dzieci, wynagrodzenie, godziny pracy i pozostałe informacje o otrzymywanym wynagrodzeniu 10 pracowników, z którymi umowy zostały rozwiązane. Administrator powiadomił tylko 10 pracowników należących do tej ostatniej grupy.

7.2.1 PRZYPADEK nr 18 – Ocena ryzyka, łagodzenie skutków i zobowiązania

129. Nawet jeśli sprawca ataku prawdopodobnie nie miał na celu gromadzenia danych osobowych, ponieważ naruszenie może prowadzić zarówno do szkód materialnych (np. strat finansowych), jak i niematerialnych (np. kradzieży tożsamości lub oszustwa), lub dane mogą zostać wykorzystane do ułatwienia innych ataków (np. phishingu), naruszenie ochrony danych osobowych prawdopodobnie spowoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych. Dlatego o naruszeniu należy poinformować wszystkich 99 pracowników, a nie tylko 10 pracowników, których informacje o wynagrodzeniach zostały ujawnione.

130. Po uzyskaniu informacji o naruszeniu administrator wymusił zmianę hasła do zagrożonych kont, zablokował wysyłanie wiadomości e-mail na konto poczty elektronicznej atakującego, powiadomił dostawcę usług poczty elektronicznej używanej przez atakującego o jego działaniach, usunął reguły ustanowione przez atakującego i udoskonalił alerty systemu monitorowania, tak aby alert był wysyłany natychmiast po utworzeniu automatycznej reguły. Alternatywnie administrator może odebrać użytkownikom prawo do ustalania reguł przekierowania, wymagając, aby zespół obsługi informatycznej robił to tylko na żądanie, lub wprowadzić zasadę, że użytkownicy powinni sprawdzać i zgłaszać reguły ustawione na ich kontach raz w tygodniu lub częściej w obszarach, w których przetwarzane są dane finansowe.

131. Fakt, że do naruszenia mogło dojść i że nie zostało ono wykryte przez tak długi czas, a także to, że w dłuższym okresie do zmiany większej ilości danych można było wykorzystać inżynierię społeczną, uwypuklił istotne problemy w systemie bezpieczeństwa informatycznego administratora. Należy niezwłocznie zająć się tymi kwestiami, np. kładąc nacisk na przeglądy automatyzacji i kontrole zmian oraz środki wykrywania incydentów

i reagowania na nie. Na administratorach danych, którzy przetwarzają dane wrażliwe, informacje finansowe itp. spoczywa większa odpowiedzialność za zapewnienie odpowiedniego bezpieczeństwa danych.

Działania konieczne w oparciu o zidentyfikowane ryzyko		
Dokumentacja wewnętrzna	Zgłoszenie organowi nadzorczemu	Zawiadomienie osób, których dane dotyczą
✓	✓	✓