BEZPIECZEŃSTWO DANYCH W PLACÓWKACH OCHRONY ZDROWIA

PRZEWODNIKI PO CYFROWEJ OCHRONIE ZDROWIA

SZYBKI START
- 8 zasad cyberbezpieczeństwa
- Gotowe wzorce dokumentacji
- RODO w ochronie zdrowia

UWAGA! CYBERATAK
- Jak działają cyberprzestępcy?
- Jak reagować w przypadku wycieku danych osobowych i medycznych?

KIEDY UODO NAKŁADA KARĘ?
- Wnioski ze sprawozdania UODO
- Upomnienia i grzywny – jak ich uniknąć?

RODO W PRAKTYCE
- Anonimizacja a pseudomizacja danych
- Procedura przeprowadzenia testu równowagi przez administratora danych osobowych

ZAGROŻENIA PODCZAS COVID-19
- Nowe niebezpieczeństwa związane z pandemią koronawirusa, o których należy pamiętać

NOWOŚCI CYFRYZACJI OCHRONY ZDROWIA

BLOG OSOZ

WWW.BLOG.OSOZ.PL

PARTNEREM SERII JEST **KAMSOFT S.A.**

KAMSOFT S.A.

Zarządzaj obiegiem EDM z **KS-EDM Suite**

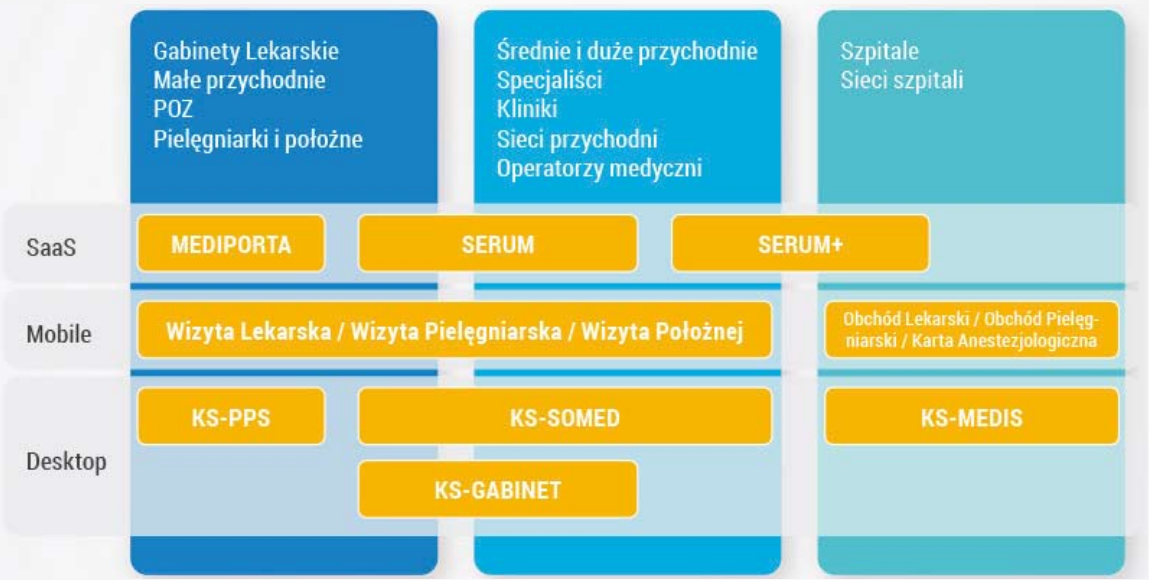
- ✓ Indeksuj i udostępniaj Elektroniczną Dokumentację Medyczną
- ✓ Raportuj Zdarzenia Medyczne
- ✓ Sprawniej i szybciej realizuj szczepienia przeciw COVID-19 i grypie
- ✓ Chroń dane przed ich uszkodzeniem lub utratą.

wejdź na:
edm.kamsoft.pl

KS-EDM SUITE | KAMSOFT SA

Nie masz jeszcze systemu do wytwarzania **EDM**?

Wybierz oprogramowanie dopasowane do Twojej placówki medycznej.



medycyna@kamsoft.pl | tel. (+48) 32 209 07 05

edm.kamsoft.pl

Czy dobrze chronisz dane?

W nowym raporcie czasopisma OSOZ Polska tłumaczymy, jak zabezpieczyć dane w placówkach ochrony zdrowia, zarówno te przechowywane w formie papierowej, jak i elektronicznej.

KAROLINA SZUCK
Inspektor Ochrony Danych
KAMSOFT S.A.

redakcja@osoz.pl

Podmioty medyczne przetwarzają niezwykle wrażliwe dane – dane o zdrowiu. Dlatego menedżerowie oraz wszyscy pracownicy ochrony zdrowia powinni być świadomi, że kwestie bezpieczeństwa informacji będą miały coraz większy wpływ na ich codzienne obowiązki. Stąd ważne jest, aby monitorować trendy wynikające z dynamicznie zmieniającego się otoczenia cybernetycznego.

Liczba cyberataków na podmioty ochrony zdrowia gwałtownie rośnie. Cyberprzestępcy stosują wyrafinowane metody i techniki kradzieży danych. A każda luka w systemach bezpieczeństwa może nie tylko doprowadzić do wycieku danych, ale także zagraża zdrowiu i życiu pacjentów. Nie wspominając o ogromnym stresie personelu administracyjnego oraz medycznego.

Digitalizacja oferuje ogromne korzyści dla ochrony zdrowia i pomaga chronić dokumentację medyczną. Dobrze zabezpieczone systemy IT, odpowiednie procedury pracy, regularne wykonywanie kopii zapasowych, systematyczne podnoszenie kompetencji cyfrowych personelu pozwolą spokojnie korzystać z wszystkich zalet dokumentów elektronicznych, jednocześnie zapewniając wysoki poziom bezpieczeństwa informacji i ochrony danych osobowych.

Placówki medyczne mają do dyspozycji cały szereg instrumentów skutecznie podnoszących poziom ochrony danych. Podstawowym jest spełnienie wymagań wynikających z RODO oraz prawidłowe zabezpieczenia na poziomie systemów informatycznych do gromadzenia i przetwarzania dokumentacji medycznej. Wśród nich warto rozważyć nowe rozwiązania, przykładowo pozwalające na automatyczne wykonywanie kopii zapasowych w chmurze danych.

Niniejszy raport jest zbiorem artykułów publikowanych w ostatnim roku w czasopiśmie o digitalizacji ochrony zdrowia – OSOZ Polska. Aktualne wskazówki znajdziecie Państwo w nowych wydaniach magazynu oraz na blog.osoz.pl.

Wiedza, którą zyskasz po przeczytaniu raportu:

- Stosowanie przepisów RODO w praktyce
- Analiza zagrożeń cyberbezpieczeństwa i ich niwelowanie
- Metody ustawicznego podwyższania kompetencji cyfrowych
- Kluczowe zasady zabezpieczenia danych
- Ważne wnioski z kar i upomnień nałożonych przez UODO
- Wpływ pandemii COVID-19 na cyberprzestępczość.

Zobacz nasze szkolenie on-line dotyczące bezpieczeństwa danych w placówkach ochrony zdrowia

Wejdź na stronę
https://bit.ly/3CgyUwf
lub zeskanuj kod

Spis treści

POLUB!

SUBSKRYBUJ!

Dołącz **do nas**

i bądź na bieżąco

- ✓ Informacje z Rynku Ochrony Zdrowia
- ✓ Nowości w systemach KAMSOFT
- ✓ Filmy szkoleniowe

Zasady prawidłowego zabezpieczenia danych w placówkach ochrony zdrowia

Konsekwencje wycieku danych medycznych w podmiocie ochrony zdrowia są zawsze dotkliwe. Oprócz kar finansowych trzeba liczyć się z szantażem cyberprzestępców, zablokowaniem systemu IT, paraliżem pracy, kryzysem wizerunkowym, nakładami finansowymi na usuwanie skutków naruszenia prywatności. Tłumaczymy, jak w prosty sposób wykonać pierwsze kroki do prawidłowego zabezpieczenia danych.

»Kodeks postępowania dla sektora ochrony zdrowia zawiera gotowe szablony dokumentów, np. wzór zgody na przetwarzanie danych osobowych, metodyka analizy ryzyka, wykaz zabezpieczeń systemów IT.«

Zagwarantowanie bezpieczeństwa informacji w placówkach ochrony zdrowia to niełatwe wyzwanie. Mają z tym problem nawet doświadczeni administratorzy szpitalnych systemów IT. W gąszczu przepisów i wymagań trudno też odnaleźć się lekarzom prowadzącym indywidualne praktyki lekarskie, którym brakuje czasu na czynności administracyjne.

Wejście w życie ogólnego rozporządzenia o ochronie danych (RODO) narzuciło nowe wymagania, które nadal dla wielu podmiotów pozostają wyzwaniem. Jakby było tego mało, rosnąca skala cyberataków powoduje, że zabezpieczenia trzeba systematycznie aktualizować i wzmacniać. Spróbujmy uporządkować wiedzę w tym zakresie.

Istnieją trzy bazowe dokumenty, które placówki medyczne powinny poznać w pierwszej kolejności:
– Kodeks postępowania dla sektora ochrony zdrowia,
– Kodeks postępowania RODO dla małych placówek medycznych,
– Przewodnik po RODO w służbie zdrowia.

Wspomniane dokumenty zawierają cenne wskazówki i spis dobrych praktyk w zakresie zapewnienia zgodności z wymogami RODO oraz ciągłego podnoszenia poziomu bezpieczeństwa informacji w placówkach ochrony zdrowia. Co ważne, obydwa kodeksy uzyskały pozytywną opinie Prezesa Urzędu Ochrony Danych Osobowych.

Podsumujmy najważniejsze zasady, które stanowią absolutne minimum w każdym podmiocie przetwarzającym dane medyczne.
1. Analiza ryzyka, identyfikacja zagrożeń oraz adekwatnych środków technicznych, fizycznych i organizacyjnych oraz podnoszenie świadomości w organizacji;
2. Dokonywanie regularnych pen-testów, ciągłe doskonalenie stosowanych zabezpieczeń dla zagrożeń związanych z cyberprzestępczością;
3. Wykonywanie regularnych kopii danych i szyfrowanie danych.

Zapewnienie rozliczalności

Zapewnienie rozliczalności przestrzegania obowiązujących przepisów realizo-

wane jest m.in. poprzez prowadzenie dokumentacji ochrony danych osobowych zawierającej procedury, instrukcje, wytyczne oraz inne uregulowania związane z bezpieczeństwem informacji.

Na dokumentację ochrony danych osobowych w placówce medycznej powinny się składać przynajmniej następujące elementy:
- szacowanie ryzyka – z niego powinno wynikać, jakie zabezpieczenia należy wdrożyć, aby zapewnić odpowiedni poziom bezpieczeństwa przetwarzanych danych;
- rejestr czynności przetwarzania;
- ewidencja naruszeń ochrony danych osobowych;
- sposób postępowania z naruszeniami ochrony danych osobowych;
- procedura rozpatrywania wniosków osób, których dane dotyczą np. w sprawie dostępu do danych, żądania usunięcia danych, kopii danych;
- procedura udostępniania dokumentacji lub informacji medycznych;
- zasady pracy w systemach informatycznych.

Umowy powierzenia

Jednym z obowiązków nakładanych przez RODO jest zawieranie umów powierzenia przetwarzania danych w trybie udostępniania danych podmiotom zewnętrznym będących Podmiotami Przetwarzającymi.

W takich umowach mamy dwie strony: *Administratora Danych Osobowych* określającego cele i sposoby wykorzystania danych osobowych oraz *Podmiot Przetwarzający* realizujący zlecenie Administratora i przetwarzający dane wyłącznie w celach wskazanych przez Administratora.

Obowiązek informacyjny

Klauzule zawierające informacje o przetwarzaniu danych, które powinny być udostępnione w taki sposób, aby pacjenci mieli możliwość się z nimi zapoznać. W praktyce wystarczy wywiesić obowiązek informacyjny w widocznym miejscu placówki medycznej oraz na stronie www (jeżeli istnieje).

Poszanowanie intymności i godności pacjentów

O poszanowaniu intymności i godności pacjentów należy pamiętać już na etapie rejestracji oraz kiedy pacjent oczekuje na wizytę w poczekalni. Obsługa pacjentów powinna odbywać się w sposób, który gwarantuje, że osoby postronne nie będą w stanie wejść w posiadanie informacji, które nie są dla nich przeznaczone. Przykładowo, inni pacjenci nie mogą dowiedzieć się, że pacjent A – wywołany z imienia i nazwiska – leczy się u lekarza danej specjalności. Oto kilka prostych sposobów, jak to zrobić:
- umieszczenie przy rejestracji informacji *„Przy stanowisku rejestracji może przebywać tylko jedna osoba”*;
- umieszczenie na podłodze przed rejestracją linii określającej strefę, poza którą czekają na swoją kolej inni pacjenci;
- stworzenie bezpiecznego sposobu wyczytywania pacjentów, np. poprzez system numerów.

Więcej zaleceń związanych z poszanowaniem prywatności pacjentów znajdą Państwo m.in. w dokumencie *Przewodnik po RODO w służbie zdrowia*.

Zabezpieczenie danych przechowywanych w formie elektronicznej

Tego typu zabezpieczenia powinny gwarantować, że osoby nieupoważnione nie będą mogły uzyskać dostępu do systemu gromadzącego dokumentację medyczną. Część środków bezpieczeństwa jest uzależniona od konkretnego systemu informatycznego i zastosowanych technologii. Istnieją jednak ogólne zalecenia, które powinny być zawsze przestrzegane:
- Odpowiednia polityka haseł – skomplikowane, długie hasła dostępu składające się z małych i dużych liter, cyfr i znaków specjalnych);
- Odpowiednia polityka czystego pulpitu oraz blokowanie stacji po określonym czasie bezczynności,
- Wykonywanie i zabezpieczanie kopii zapasowych zbiorów danych;
- Stosowanie kryptograficznych środków ochrony przetwarzanych danych osobowych przez osoby użytkujące komputer przenośny zawierający dane osobowe podczas transportu;
- Zabezpieczenia fizyczne kluczowej infrastruktury;
- Wykorzystanie agregatów prądotwórczych, urządzeń UPS;
- Zabezpieczanie elektronicznych nośników informacji;
- Wykorzystywanie systemów antywirusowych;
- Używanie aktualnych wersji oprogramowania aplikacyjnego;
- Szkolenia pracowników w zakresie zapobiegania atakom socjotechnicznym;
- Przeprowadzanie testów bezpieczeństwa systemu w tym testów penetracyjnych.

Należy pamiętać, że wszystkie zabezpieczenia powinny wynikać z przeprowadzonego szacowania ryzyka.

Zabezpieczenie papierowej dokumentacji medycznej

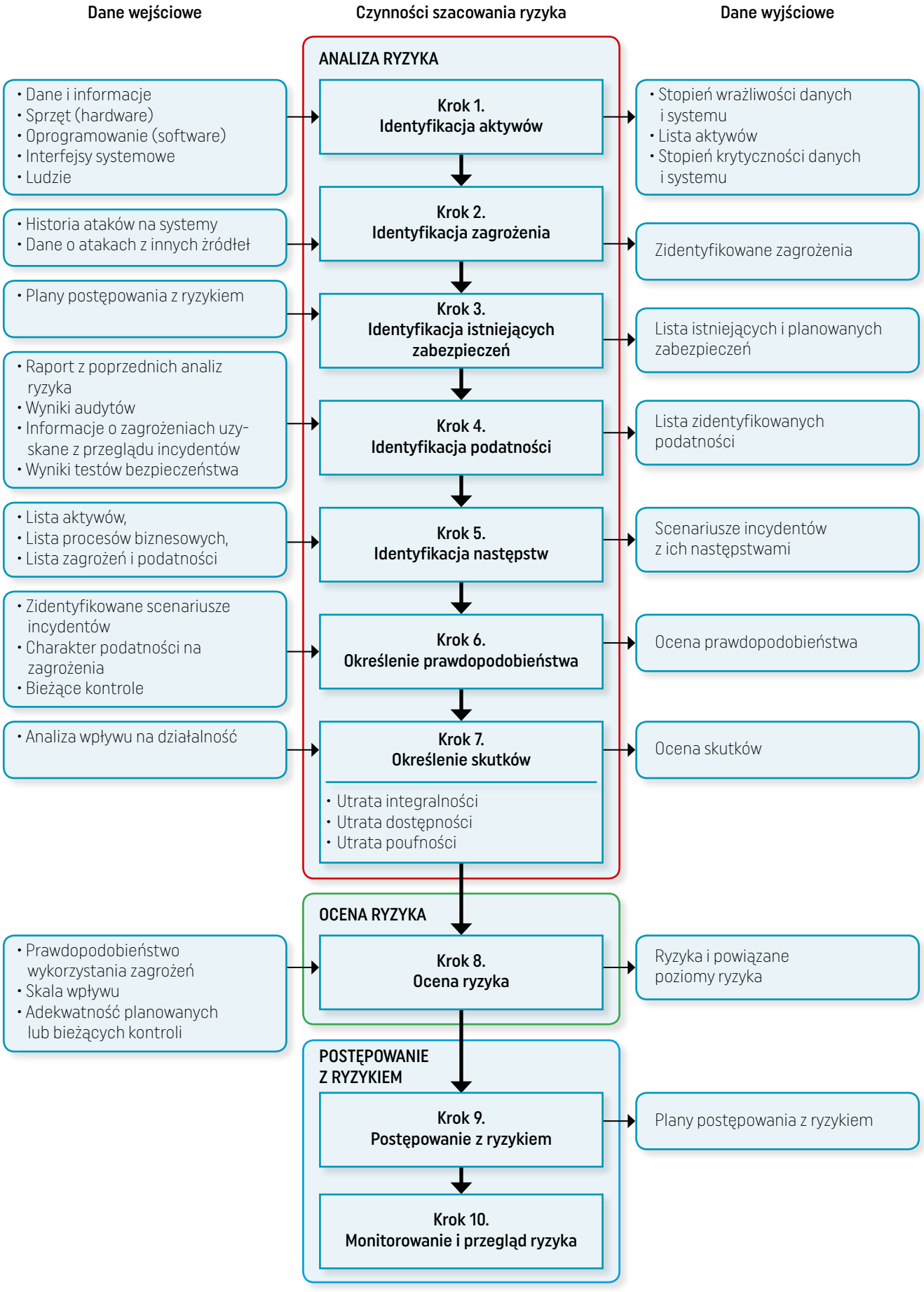
Nie istnieje jedno, uniwersalne rozwiązanie – zabezpieczenia zawsze powinny wynikać z przeprowadzonego szacowania ryzyka oraz możliwości lokalowych podmiotu. Jednak przeprowadzając analizę należy wziąć pod uwagę zagrożenia związane z:
- kradzieżą dokumentacji papierowej. Można ją minimalizować wprowadzając rolety, kraty, systemy antywłamaniowe i alarmowe;
- nieuprawnionym dostępem z wewnątrz osób spoza personelu medycznego. Wśród najprostszych sposobów można wymienić przechowywanie kartotek w szafach zamykanych na klucz, a także zarządzanie kluczami do pomieszczeń;
- brakiem dostępu do gromadzonej dokumentacji. Aby zapobiec zniszczeniu dokumentów, warto zapewnić optymalne warunki środowiskowe, takie jak optymalna temperatura, wilgotność, wentylacja, systemy alarmujące zagrożenia jak zalanie albo pożar.

Szkolenia i aktualizacja wiedzy

Zastosowanie wyłącznie środków technicznych i organizacyjnych to dopiero pierwszy krok. Drugim jest dostarczenie personelowi informacji o tym, jak pracować z danymi osobowymi, z jakimi zagrożeniami mogą się spotkać, jak na nie reagować. Personel musi być szkolony z obowiązujących w placówce zasad bezpieczeństwa i ochrony danych osobowych. Powinien wiedzieć, jakimi metodami posługują się cyberprzestępcy próbujący wykraść dane lub zainfekować komputer. Generalna zasada brzmi: system zabezpieczeń danych osobowych w placówce medycznej jak tak mocny, jak jego najsłabsze ogniwo.

Upoważnienia osób zatrudnionych

Każda osoba zatrudniona w placówce medycznej powinna mieć ściśle określony dostęp do danych osobowych. Zakres upoważnień powinien uwzględniać obowiązki osoby zatrudnionej. Warto pamiętać, aby nie nadawać personelowi uprawnień „na zapas”, w sposób nadmiarowy. Istotne jest także prawidłowe ewidencjonowanie osób upoważnionych do przetwarzania danych osobowych. ●


Dane wejściowe
Czynności szacowania ryzyka
Dane wyjściowe
ANALIZA RYZYKA
• Dane i informacje
• Sprzęt (hardware)
• Oprogramowanie (software)
• Interfejsy systemowe
• Ludzie
Krok 1.
Identyfikacja aktywów
• Stopień wrażliwości danych i systemu
• Lista aktywów
• Stopień krytyczności danych i systemu
• Historia ataków na systemy
• Dane o atakach z innych źródłeł
Krok 2.
Identyfikacja zagrożenia
Zidentyfikowane zagrożenia
• Plany postępowania z ryzykiem
Krok 3.
Identyfikacja istniejących zabezpieczeń
Lista istniejących i planowanych zabezpieczeń
• Raport z poprzednich analiz ryzyka
• Wyniki audytów
• Informacje o zagrożeniach uzyskane z przeglądu incydentów
• Wyniki testów bezpieczeństwa
Krok 4.
Identyfikacja podatności
Lista zidentyfikowanych podatności
• Lista aktywów,
• Lista procesów biznesowych,
• Lista zagrożeń i podatności
Krok 5.
Identyfikacja następstw
Scenariusze incydentów z ich następstwami
• Zidentyfikowane scenariusze incydentów
• Charakter podatności na zagrożenia
• Bieżące kontrole
Krok 6.
Określenie prawdopodobieństwa
Ocena prawdopodobieństwa
• Analiza wpływu na działalność
Krok 7.
Określenie skutków
• Utrata integralności
• Utrata dostępności
• Utrata poufności
Ocena skutków
OCENA RYZYKA
• Prawdopodobieństwo wykorzystania zagrożeń
• Skala wpływu
• Adekwatność planowanych lub bieżących kontroli
Krok 8.
Ocena ryzyka
Ryzyka i powiązane poziomy ryzyka
POSTĘPOWANIE Z RYZYKIEM
Krok 9.
Postępowanie z ryzykiem
Plany postępowania z ryzykiem
Krok 10.
Monitorowanie i przegląd ryzyka

Śledź aktualne wskazówki na temat cyberbezpieczeństwa na blogu OSOZ.

Nowy blog o e-zdrowiu

Praktyczne porady
Informacje z rynku zdrowia
Inspirujące wywiady

BLOG OSOZ
blog.osoz.pl

ZESKANUJ KOD,
aby przejść do bloga


Zdjęcie nstytut CyberPeace

Cyberataki na placówki zdrowia są atakami na zdrowie i życie pacjentów

Raport „Igranie życiem: Cyberataki na służbę zdrowia to ataki na ludzi" (Playing with Lives: Cyberattacks on Healthcare are Attacks on People) uświadamia skalę problemu ataków hakerskich, naruszeń danych i operacji dezinformacyjnych w służbie zdrowia oraz pokazuje, jak ogromne zagrożenie stanowią one dla zdrowia i życia ludzi. Dokument zawiera ponadto listę rekomendacji, jak przeciwdziałać cyberprzestępczości.

Globalna pandemia COVID-10 obnażyła istniejące słabości systemu ochrony zdrowia w zakresie cyberprzestępczości. Niestety, systemy ochrony zdrowia w niewystarczającym stopniu reagują na zagrożenie bezpieczeństwa danych, czego przykładem są m.in. najbardziej niszczycielskie w ostatnich latach cyrberataki WannaCry i NotPetya.

W 2017 roku, WannaCry zaatakował ponad 600 podmiotów medycznych brytyjskiej służby zdrowia, zakłócając dostęp do krytycznych informacji oraz powodując konieczność ograniczenia liczby wizyt. Niemniej jednak, 4 lata po tych wydarzeniach nie widać wyraźnej poprawy w kwestii ochrony infrastruktury IT ochrony zdrowia. Jednocześnie skala zagrożeń nieustannie rośnie, a „infodemia" związana z pandemią COVID-19 jedynie dodatkowo je potęguje.

Opieka zdrowotna potrzebuje cyberpokoju. Musi być wolna od wszelkich zagrożeń, tak aby placówki medyczne mogły działać bez zakłóceń, czyli bez przerw w dostępie do danych kluczowych w opiece nad pacjentem.

Ataki na służbę zdrowia powodują bezpośrednie szkody dla ludzi i stanowią zagrożenie dla zdrowia w skali globalnej

Kiedy atakowane są podmioty świadczące usługi opieki zdrowotnej, ofiarami nie jest tylko infrastruktura IT, ale przede wszystkim ludzie – pracownicy służby zdrowia i pacjenci. Zakłócenia pracy systemów informatycznych wpływają na proces opieki, wiążą się z dużymi kosz-

tami dla budżetów szpitali, a takie skutki uboczne jak psychologiczne szkody wywołane kradzieżą prywatnych informacji przez przestępców mogą być ogromne.

Utrata dostępu do dokumentacji medycznej i urządzeń medycznych ratujących życie stanowi poważne zakłócenie dla płynności działania szpitali. Cyberataki podkopują także zaufanie społeczne do procesu digitalizacji, które oferuje szereg korzyści. Wielu menedżerów podmiotów ochrony zdrowia, w obawie o wyciek danych, hamuje inwestycje w cyfryzację, co w perspektywie długofalowej jest szkodliwą strategią.

Ataki nasilają się i ewoluują. Hakerzy wykorzystują słabe punkty delikatnej infrastruktury cyfrowej sektora opieki zdrowotnej oraz słabości systemu bezpieczeństwa cybernetycznego

Arsenał broni wykorzystywanej do ataków na służbę zdrowia jest coraz szerszy. Pandemia COVID-19 dała początek nowym incydentom. Ośrodki badań nad szczepionkami stały się ofiarami cyberszpiegostwa; hakerzy żądają od szpitali okupu za przywrócenie stanu systemów IT sprzed ataku. Te mając na szali życie ludzkie, często decydują się uiścić opłatę; pracownicy służby zdrowia i międzynarodowe organizacje zdrowotne są celem kampanii dezinformacji i cyberataków mających na celu podważenie ich wiarygodności. Jak pokazują krajowe statystyki, liczba przypadków naruszenia danych w służbie zdrowia w 2020 r. znacznie wzrosła.

»W wyniku cyberataków może dojść do przerwania płynności funkcjonowania szpitala oraz obniżenia zaufania do digitalizacji oferującej niewątpliwe korzyści w ochronie zdrowia.«

Hakerzy wykorzystują podatne na ataki, nieraz przestarzałe środowiska cyfrowe w służbie zdrowia, w tym urządzenia medyczne i infrastrukturę IT. Wiedzą oni, że placówki medyczne mają ograniczone budżety na szczelne zabezpieczenie danych i znalezienie luk bezpieczeństwa jest o wiele łatwiejsze niż w przypadku przykładowo instytucji finansowych.

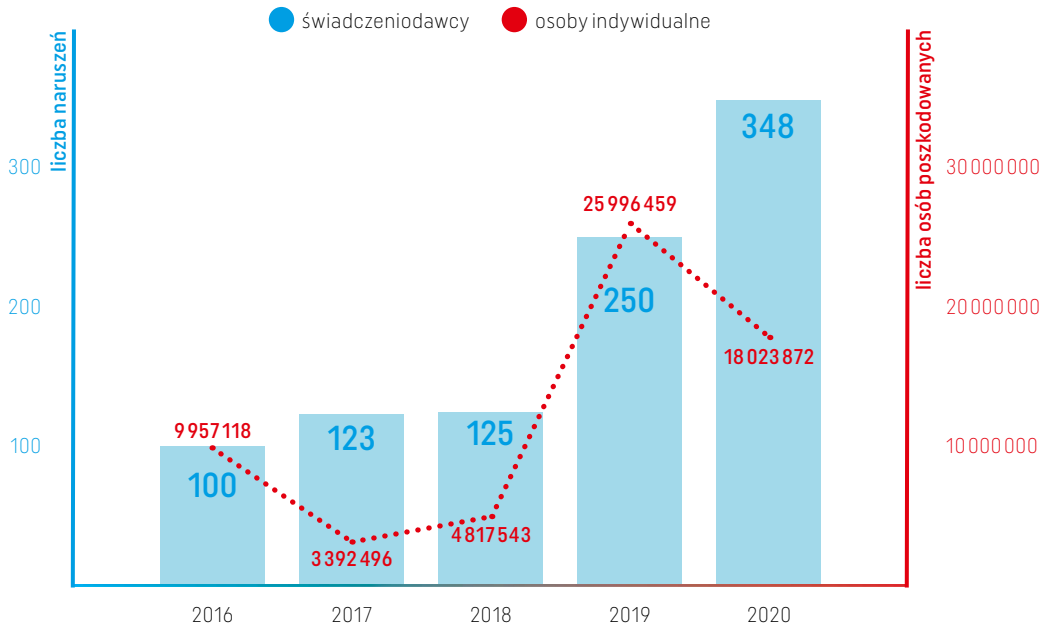
Bezpieczeństwo cybernetyczne w służbie zdrowia jest niedofinansowane. Jedynie duże podmioty sektora opieki zdrowotnej wdrożyły wysokiej jakości systemy i procedury bezpieczeństwa cybernetycznego. Niestety, większość cierpi z powodu chronicznego braku środków na zabezpieczenie infrastruktury, szkolenie personelu oraz zatrudnianie i utrzymywanie pracowników zajmujących się bezpieczeństwem cybernetycznym.

Ataki na służbę zdrowia to przestępstwa o niskim ryzyku i wysokim zysku, a hakerzy często pozostają bezkarni

Ataki na opiekę zdrowotną to lukratywny biznes. Są zjawiskiem międzynarodowym, niezależnie od tego, czy ich celem jest wymuszenie okupu od świadczeniodawców, kradzież dokumentacji medycznej i własności intelektualnej, czy też podważenie zaufania publicznego. Ponieważ organizacje opieki zdrowotnej są „strażnikami" wysoce wrażliwych informacji, sektor zdrowia jest bardzo dochodowym celem dla cyberprzestępców.

Ataki na służbę zdrowia są rzadko rejestrowane i zgłaszane do organów bezpieczeństwa. Wiele organizacji nie wie, jak postępować, gdyż nie mają odpowiednich kompetencji i procedur bezpieczeństwa cybernetycznego. Ponadto, obawa przed odpowiedzialnością karną

Naruszenia bezpieczeństwa informacji zdrowotnych w USA (2016–2020)



Źródło: CyberPeace

lub utratą reputacji utrudnia zgłaszanie incydentów bezpieczeństwa, podobnie jak brak wiary w to, że przestępcy zostaną złapani i ukarani.

Placówki nie korzystają w pełni z instrumentów prawnych i istniejących inicjatyw pomocowych

Wiele podmiotów nie wie, z jakich środków pomocowych mogą skorzystać, zarówno tych mogących zapobiec atakom, jak i tych oferowanych w przypadku wycieku danych. Pacjenci nie mają świadomości, jakie prawa im przysługują.

W przypadku cyberataków, placówki medyczne często panicznie starają się ukryć tego typu fakt, zamiast szukać wsparcia. Wynika to często z przekonania, że konkretne osoby mogą zostać posądzone o luki w procedurach bezpieczeństwa, które powinny być wdrożone i egzekwowane. Jednocześnie wiele podmiotów nadal nie wdrożyło obowiązujących wymagań nakładanych przepisami prawa takich jak RODO.

Co należy zrobić, aby wzmocnić odporność służby zdrowia na cyberataki?

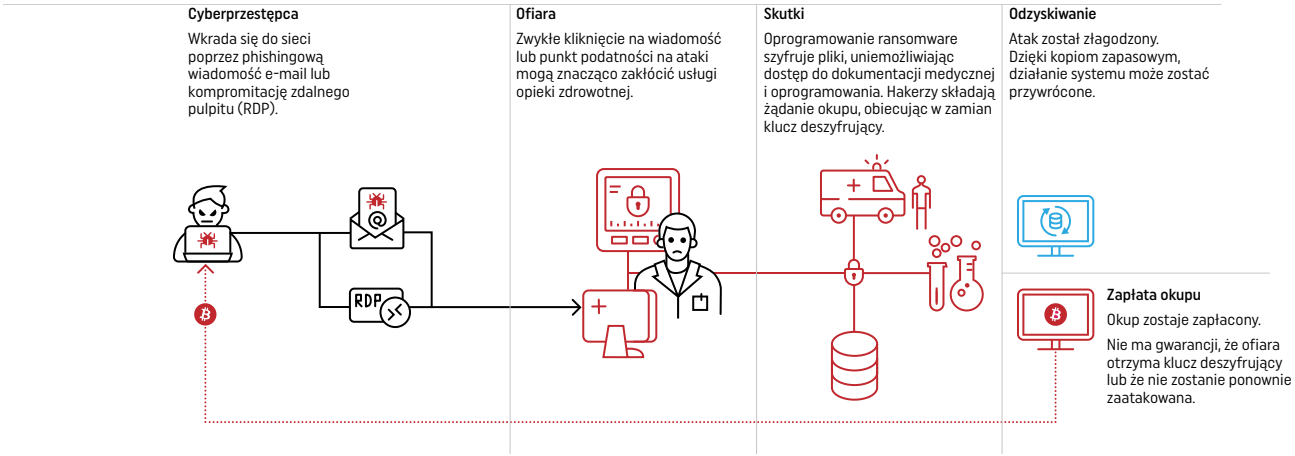
Choć zagrożenia ze strony cyberprzestępców systematycznie rosną, ochrona zdrowia nie jest wobec nich bezsilna. Po atakach WannaCry z 2017 roku, w Wielkiej Brytanii postanowiono zainwestować 150 mln funtów w bezpieczeństwo systemu narodowej służby zdrowia (NHS). Cyberbezpieczeństwo powinno być priorytetem wszystkich inwestycji w cyfryzację. Placówki medyczne potrzebują wsparcia finansowego na rozwój infrastruktury, podnoszenie kompetencji swoich pracowników. Z kolei rządy poszczególnych państw powinny konsekwentnie ścigać cyberprzestępców.

Raport „Igranie życiem: Cyberataki na służbę zdrowia to ataki na ludzi" wskazuje takie rekomendacje jak:

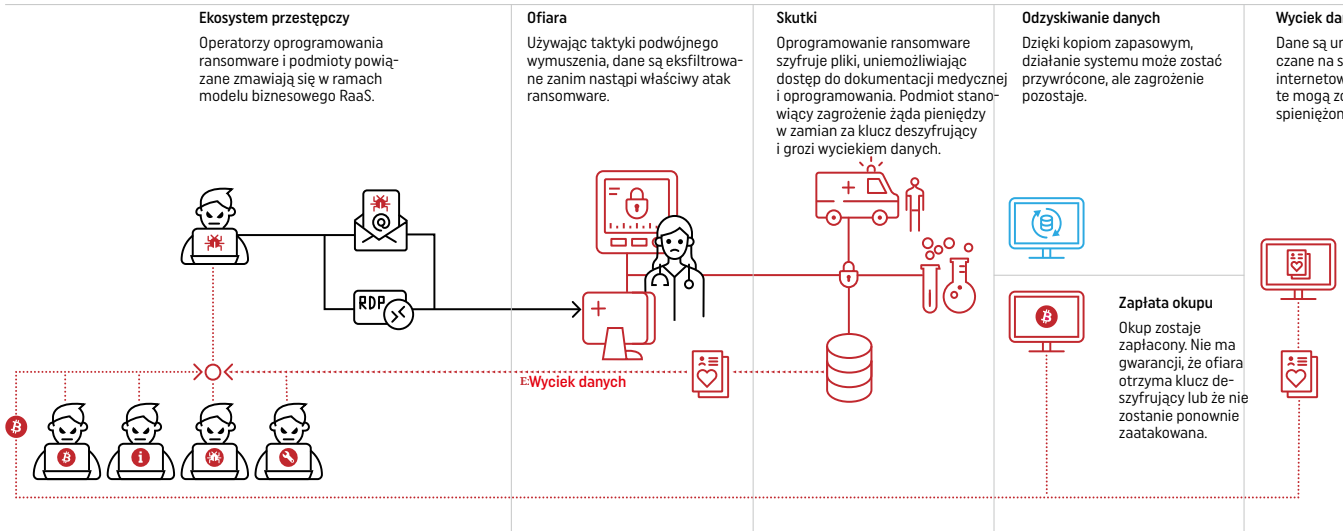
1. Szczegółowe dokumentowanie ataków i analiza ich wpływu na indywidualne podmioty, w tym ogólne skutki społeczne;

Mechanizm ataków ransomware i podwójnego wymuszenia

Ransomware



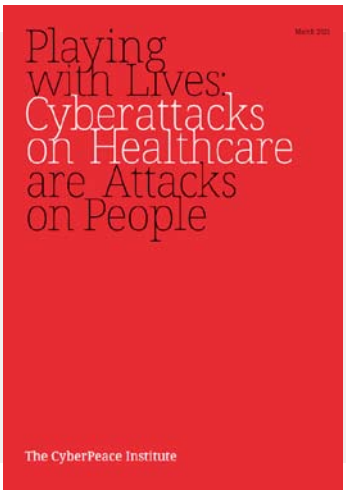
Podwójne wymuszenie



Źródło: CyberPeace

Zdjęcie nstytut CyberPeace

2. Poprawa gotowości i odporności sektora opieki zdrowotnej na cyberataki poprzez:
   - inwestycje w infrastrukturę bezpieczeństwa cybernetycznego;
   - inwestycje w rozwój umiejętności cyfrowych pracowników służby zdrowia;
   - opracowywanie i wdrażanie procedur bezpieczeństwa oraz ich systematyczny przegląd.
3. Poprawa gotowości systemu opieki zdrowotnej na ataki poprzez:
   - wdrożenie instrumentów technicznych i prawnych;
   - opracowanie wytycznych bezpieczeństwa cybernetycznego dla placówek ochrony zdrowia;
   - wyznaczenie budżetów na zapewnienie ochrony danych;
   - kampanie informacyjne;
   - współpraca międzynarodowa i wymiana doświadczeń.
4. Ściganie cyberprzestępstw w ochronie zdrowia i pociąganie do odpowiedzialności hakerów, co wymaga sprawnej współpracy organów wymiaru sprawiedliwości w skali globalnej.
5. Stworzenie kodeksu dobrych praktyk projektowania systemów IT dla ochrony zdrowia i administracyjnych z uwzględnieniem zasad „bezpieczeństwa wkomponowanego w system" oraz „bezpieczeństwa domyślnego" (and.: data protection by design and by default). Systemy IT powinny m.in. egzekwować konieczność autoryzacji dostępu do danych, wyznaczać poziomy uprawnień dostępu do określonych danych, blokować czynności mogące narażać dane na wyciek, wymuszać systematyczną archiwizację bez danych. Oprogramowanie antywirusowe należy systematycznie aktualizować, a pracownicy powinni być informowani o możliwych atakach i szkoleni z narzędzi stosowanych przez cyberprzestępców. ●



Igranie życiem: Cyberataki na ochronę zdrowia to ataki na ludzi

Playing with Lives: Cyberattacks on Healthcare are Attacks on People

Raport przygotowany przez CyberPeace Institute
(61 stron, język angielski)

Aby pobrać raport, wejdź na stronę
https://bit.ly/3pu6NVc
lub zeskanuj kod

Buduj **relacje** z pacjentami dzięki **aplikacji**

VisiMed

- ✓ Ułatwiasz pacjentom rezerwację wizyt
- ✓ Zmniejszasz kolejki i liczbę telefonów do rejestracji
- ✓ Realizujesz porady on-line i zamówienia na e-Recepty
- ✓ Redukujesz liczbę niezrealizowanych wizyt
- ✓ Dbasz o dyskrecję obsługi pacjenta

Co zrobić, aby personel placówki medycznej swobodnie posługiwał się oprogramowaniem?

Inwestując w systemy IT, każda placówka oczekuje korzyści: wysokiej jakości usług, usprawnienia procesów leczenia, szybkiego dostępu do danych. Elektroniczna dokumentacja medyczna ma ułatwiać pracę, pozwalając lekarzom więcej czasu poświęcić pacjentowi. Aby to osiągnąć, należy opracować strategię ciągłego podnoszenia kompetencji cyfrowych. Na czym ona polega?

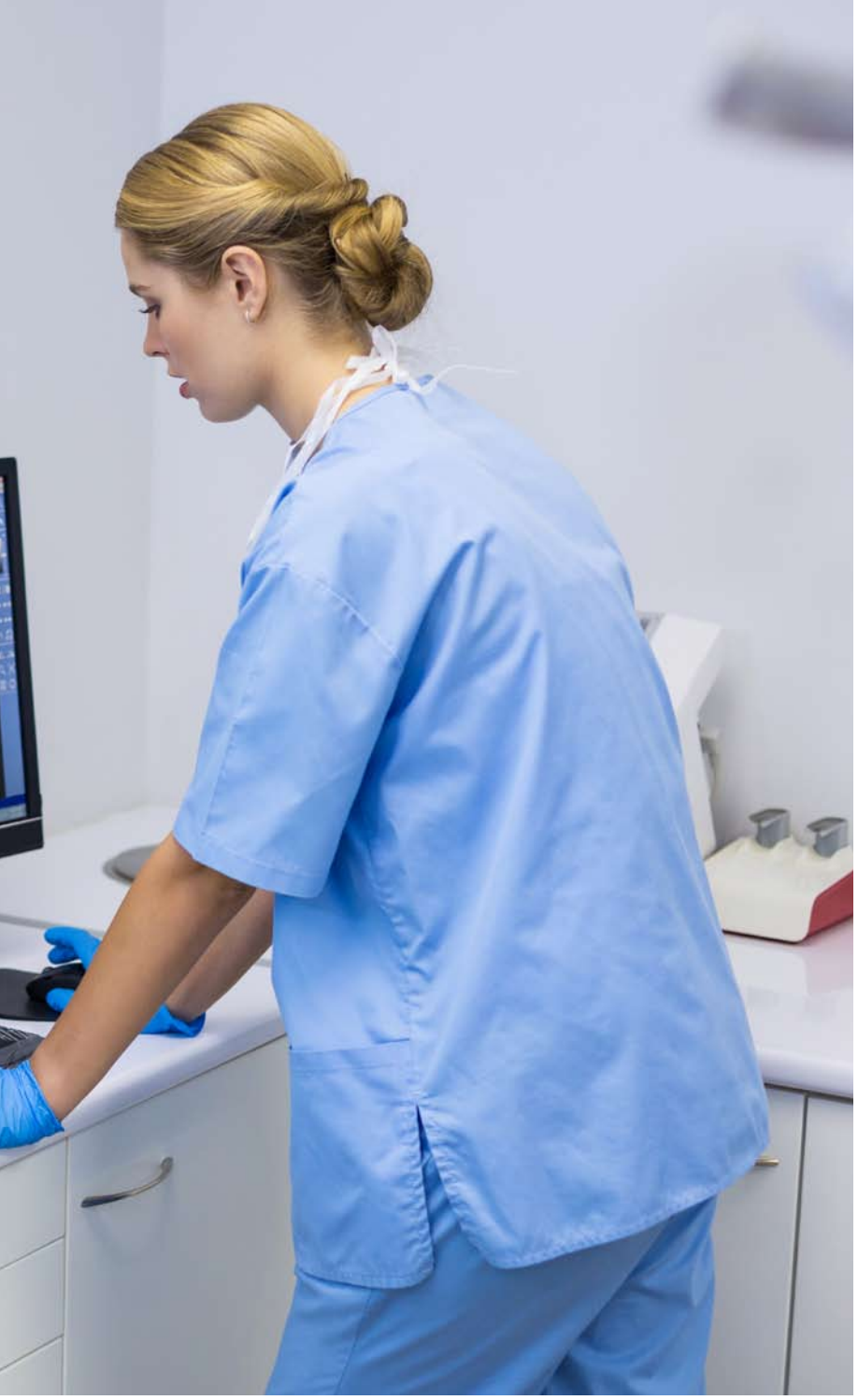
Ochrona zdrowia nadrabia zaległości cyfrowe w stosunku do innych branż. Z punktu widzenia lekarza, pielęgniarki czy personelu administracyjnego oznacza to konieczność nauki wielu nowych funkcjonalności systemów IT w krótkim czasie. Do tego trzeba dodać bieżące zmiany w oprogramowaniu wynikające z nowych przepisów administracyjnych, modyfikacji sposobu rozliczeń z płatnikami, obowiązków sprawozdawczych.

Nie zapominajmy, że personel medyczny często pracuje w różnych placówkach medycznych, a więc musi w ciągu jednego dnia obsługiwać różne programy. Na to wszystko nakłada się duża rotacja kadr oraz zróżnicowanie umiejętności wyjściowych pomiędzy młodymi medykami sprawnie posługującymi się komputerem, smartfonem i tabletem, a starszym personelem przyzwyczajonym do dokumentów papierowych.

Zmienia się też sama technologia – organizacje przechodzą na rozwiązania chmurowe, komputery stacjonarne zastępowane są urządzeniami mobilnymi, dokumentacja coraz częściej notowana jest głosowo, systemy wspomagania decyzji klinicznych narzucają nowe procedury pracy.

Jak nad tym zapanować, pamiętając, że umiejętności cyfrowe wpływają na jakość EDM, precyzję rozliczeń a przez to sytuację finansową, bezpieczeństwo pacjenta i cyberbezpieczeństwo placówki?

Systematycznie aktualizowane systemy IT, unowocześniany na bieżąco sprzęt medyczny i komputerowy – to,



czy pracownicy odnajdą się w szybko zmieniających się warunkach, zależy od dobrze zaplanowanego programu stałego podnoszenia kompetencji. Składa się on z sześciu filarów:

1. Zdefiniowanie mierzalnych elementów umiejętności;
2. Komunikacja celów oraz harmonogramu digitalizacji;
3. Zaplanowanie szkoleń dopasowanych do różnych grup;
4. Systematyczne podnoszenie kompetencji cyfrowych;
5. Ocena umiejętności cyfrowych;
6. … oraz ich doskonalenie.

Jak mierzyć umiejętności?

Pierwszy punkt może okazać się kluczowy. Na tym etapie trzeba oddzielić miękkie elementy, jak swoboda obsługi komputera, szybkość wprowadzania danych do systemu czy zdolność ułatwiania własnej pracy przez odpowiednie ustawienia opcji systemów IT. Te elementy powinny podlegać obserwacji i być częścią systematycznego podnoszenia kompetencji, ale nie są pierwszoplanowe. Mierzenie szybkości wprowadzania danych pacjenta do systemu byłoby chyba najgorszym pomysłem prowadzącym jedynie do szkodliwej presji psychicznej.

Kontrolować należy przede wszystkim elementy decydujące o kluczowych wskaźnikach: bezpieczeństwie pacjenta, sytuacji finansowej, jakości usług. Miernikami może być systematyczny przegląd jakości wprowadzanych danych i audyty.

Zarządzanie zmianą cyfrową

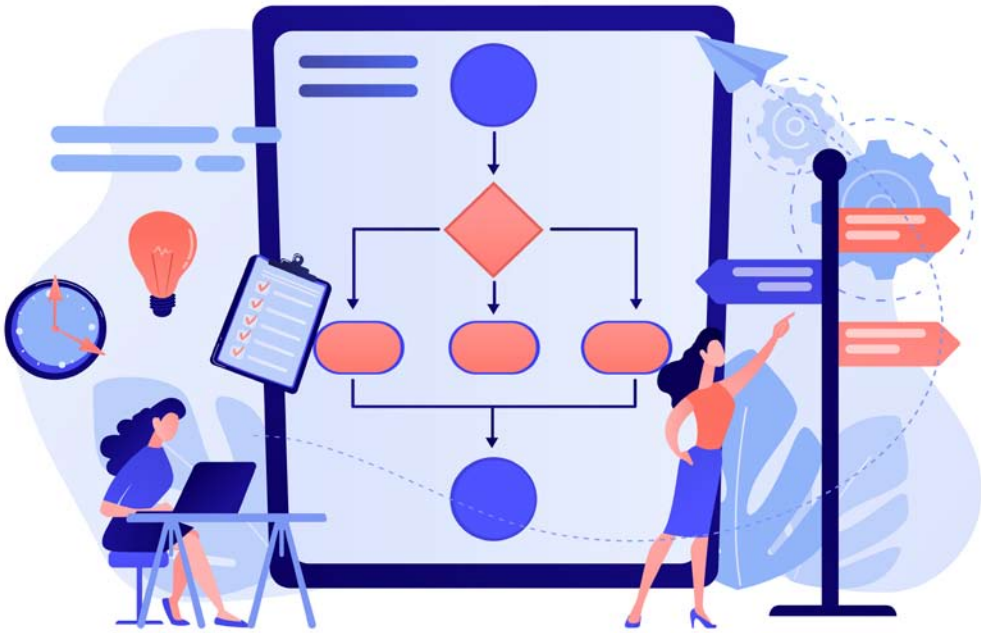
Strategicznym elementem jest komunikowanie personelowi, po co wprowadza się nowy system. A jeszcze lepiej – włączenie pracowników w proces projektowania zmian, aby czuli się ich częścią, dostrzegając sens innowacji. Poprawa koordynacji leczenia czy sytuacji finansowej są argumentami bardziej przekonującymi niż ogólne sformułowana „cyfryzacja."

W ramach „onboardingu", czyli oswajania nowych pracowników z IT, punktem wyjścia jest ankieta pozwalająca poznać umiejętności bazowe. Na tej podstawie można wyróżnić różne grupy i dopasować do nich odpowiedni cykl szkoleń. Podnoszenie umiejętności cyfrowych, a tym samym innowacyjności, powinno stać się częścią kultury organizacyjnej.

Szkolenia, indywidualne porady

Za wprowadzeniem każdej nowej funkcjonalności systemu powinna iść wiedza – szkolenie na danych testowych, dobrze przygotowana dokumentacja. W systemie szkoleń trzeba przewidzieć różne programy, od ogólnych warsztatów grupowych prowadzonych przez producenta oprogramowania, po spotkania indywidualne, webinary online do samodzielnej nauki w dowolnym czasie. W razie pilnych pytań, aby nie doprowadzić do blokady pracy, pracownik musi mieć możliwość szybkiego skontaktowania się z ekspertem poprzez czat z działem IT lub rozmowę z opiekunem wyznaczonym ze strony producenta/firmy IT.

Seria szkoleń z nowego systemu to dopiero początek. Każda organizacja potrzebuje strategii ciągłego podnoszenia kompetencji. W dużych organizacjach jak szpitale, najlepiej sprawdza się wyznaczenie lidera, który płynnie porusza się w infrastrukturze IT i na podstawie obserwacji pracy pracowników zgłasza kierownictwu sugestie dotyczące podnoszenia kompetencji. Tego rodzaju coach



»Niektóre umiejętności cyfrowe decydują o bezpieczeństwie pacjenta oraz danych.«

jest najbliżej pracownika i może na bieżąco odpowiadać na pilne pytania.

Umiejętności cyfrowe warto systematycznie mierzyć. Nie po to, aby kontrolować czy karać pracowników, ale by rozwijać ich kompetencje ułatwiając codzienne wykonywanie obowiązków. Każdy zgodzi się z tym, że płynna obsługa systemu IT wpływa pozytywnie na zadowolenie na stanowisku pracy. Z kolei brak umiejętności cyfrowych może być nie tylko frustrujący, ale też niebezpieczny prowadząc do wypalenia zawodowego.

Do absolutnego minimum pomiarów umiejętności należą audyty bezpieczeństwa cybernetycznego prowadzone przez dział IT. Czy pracownik otwiera podejrzane e-maile i klika na zawarte w nich linki? Czy wylogowywuje się z systemu podczas przerwy?

Praca z IT, która sprawia przyjemność

W ostatnich latach obserwujemy duży postęp w ergonomii systemów IT. Producenci na bieżąco dopasowują je do oczekiwań użytkownika, wprowadzają nowe interfejsy, udostępniają wersje systemów do wygodnej obsługi na urządzeniach mobilnych.

Jednak wartość i korzyści z każdego systemu IT zależą w pierwszej linii od wiedzy pracowników o tym, jak je obsługiwać. Warto zbudować spójną strategię podnoszenia umiejętności. Informacje na temat systemów IT, modułów, nowych funkcji muszą być ustrukturyzowane, dostępne na żądanie w lokalnej sieci, w różnym formacie – od drukowanych podręczników do filmów instruktażowych. Tak, aby każdy mógł uczyć się we własnym tempie, w sposób jaki preferuje.

Umiejętności cyfrowe nie zawsze łatwo zmierzyć, ale można je dobrze ocenić na podstawie obserwacji. Wyznaczony lider cyfryzacji w komórce organizacyjnej może zbierać osobiste spostrzeżenia dotyczące działania systemu, zgłaszanych problemów. Niektóre placówki sięgają do ankiet doświadczeń obsługi oprogramowania.

Niezbędne jest zapewnienie wsparcia w czasie rzeczywistym. Tutaj też dobrym pomysłem jest zaangażowanie wspomnianego lidera cyfryzacji – coacha. Łatwiej zapytać kolegę o wsparcie niż każdorazowo dzwonić do działu IT czy udawać, że nie ma problemu.

Odpowiedzialność za komfort pracy z systemem IT leży pomiędzy placówką medyczną a dostawcą oprogramowania. Dlatego zakup systemu IT to nie tylko transakcja, ale nawiązanie bliskiej współpracy z dostawcą. Przykładowo, firma informatyczna skorzysta na zgłaszanych przez pracowników na pierwszej linii propozycjach i będzie mogła je uwzględniać w kolejnych wersjach oprogramowania. Z kolei placówka zyskuje wpływ na kształt systemu.

I na koniec najważniejszy element – ustawiczne uczenie się. Nowy tomograf albo komputer wymaga zazwyczaj jednorazowego szkolenia z obsługi. Z kolei do oprogramowania wprowadzane są na bieżąco nowe funkcje. Wiele z nich nie jest w ogóle wykorzystywanych, a mogłyby znacznie podnieść jakość pracy. To dotyczy też szeregu opcji dostępnych w systemach – ich odpowiednia konfiguracja może spowodować zaoszczędzenie kilku sekund na rejestrowaniu danych, co przelicza się na kilkadziesiąt minut dziennie.

Organizacja, która dba o podnoszenie kwalifikacji cyfrowych, maksymalizuje też korzyści płynące z inwestycji w oprogramowanie w tym najcenniejszy z zasobów – pracowników. ●

KAMSOFT S.A.

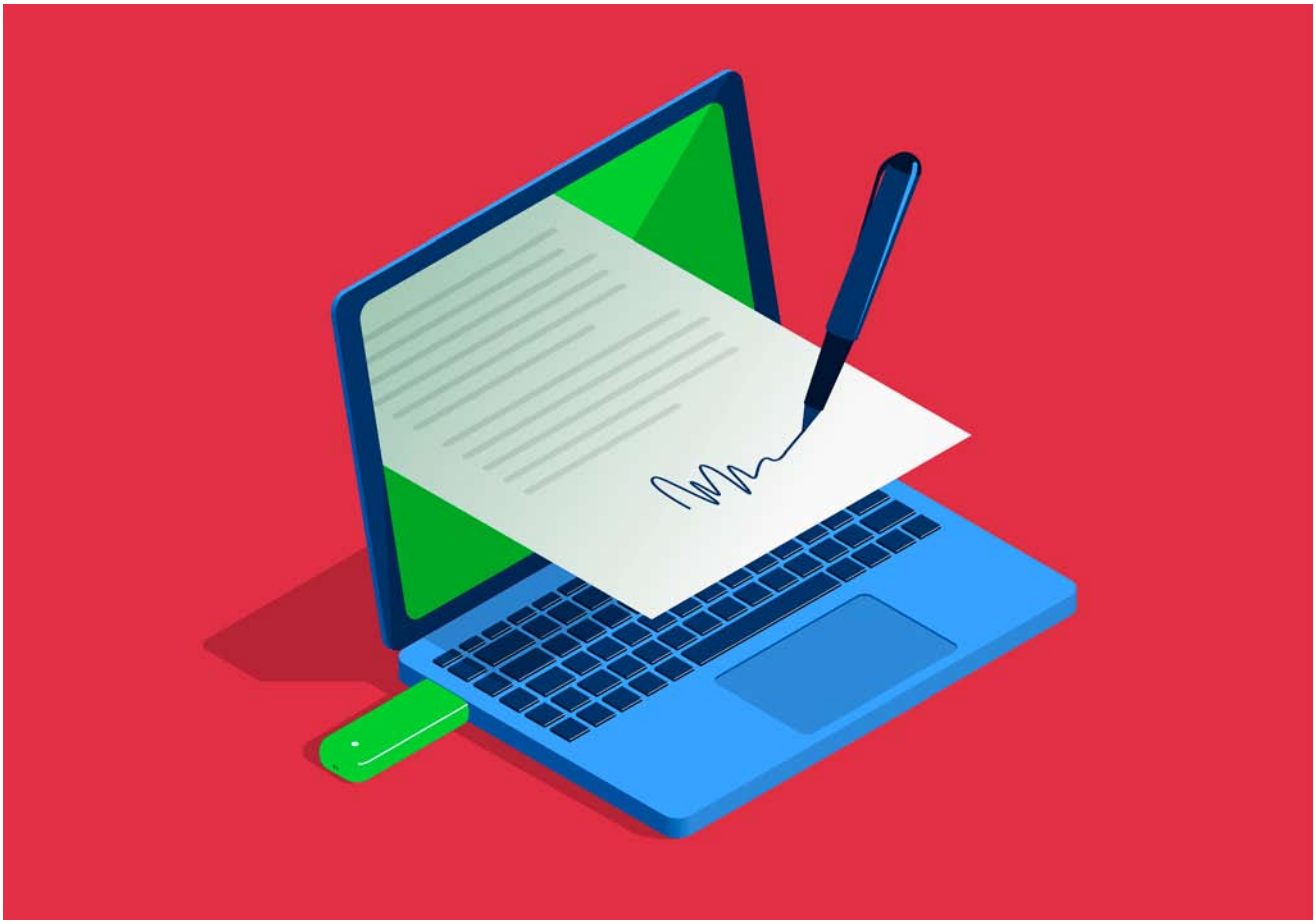
Zwiększ **bezpieczeństwo** danych w swojej **aptece**

włącz **RepoCloud** i **CopyCloud** już dziś

- ✓ **Zminimalizuj** ryzyko utraty danych
- ✓ **Zapewnij** ciągłość działania apteki
- ✓ **Odzyskuj** dane po awarii bez straty

ks-omnipharm_one@kamsoft.pl | tel. (+48) 32 209 07 05

Zobacz prezentację



Zgoda, czyli kiedy można przetwarzać dane osobowe?

Zgoda osoby, której dane dotyczą, jest jedną z określonych w RODO przesłanek legalizujących przetwarzanie danych osobowych. Niestety często jest ona wykorzystywana jako przesłanka legalizująca w procesach, w których nie ma to uzasadnienia.

W codziennej pracy Inspektora Danych Osobowych często spotykam się z błędną opinią, że jeżeli zgoda na przetwarzanie danych osobowych nie została wyrażona, administrator nie może przetwarzać danych, co sugerowałoby, że istnieje wyłącznie jedna właściwa przesłanka legalizująca. Rzecz ma się jednak zgoła inaczej, bowiem zgoda może być podstawą do przetwarzania danych, wyłącznie wtedy, gdy nie występują inne przesłanki legalizujące, które są określone w art. 6 ust. 1 RODO. Przepis ten, oprócz zgody, określa, że dane mogą być przetwarzane m.in. gdy jest to niezbędne do wykonania umowy, do wypełnienia obowiązku prawnego ciążącego na administratorze, do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a także gdy administrator musi zrealizować cel wynikający z prawnie uzasadnionych interesów.

Zgoda zebrana w przypadku istnienia innych przesłanek legalizujących może prowadzić do naruszenia zasady rzetelności i przejrzystości, o których mowa w RODO, gdyż osoba udzielająca zgody byłaby przekonana, że to na tej podstawie przetwarzane są jej dane, więc gdy zgłosi chęć wycofania zgody – administrator zaprzestanie dalszego przetwarzania. Administrator zaś może mieć wręcz obowiązek przetwarzania danych, gdy mają zastosowanie inne wyżej przedstawione przesłanki, stąd usuwając dane na podstawie żądania wycofania zgody mógłby np. naruszyć przepisy prawa zobowiązujące go do gromadzenia da-

nych, jeżeli właściwą podstawą prawną dla tego procesu byłoby wypełnienie obowiązku prawnego ciążącego na administratorze.

Wróćmy zatem do najważniejszego pytania – kiedy zgoda może stać się przesłanką legalizującą? Administrator każdorazowo jest zobowiązany do analizy procesu przetwarzania danych i dopiero gdy nie mają zastosowania wszystkie inne przesłanki, to podstawą do przetwarzania danych osobowych może być zgoda. Gdy jednak zgoda ma zastosowanie, musi ona spełniać określone warunki, by rzeczywiście mogła być podstawą przetwarzania.

Definicja zgody określona w art. 4 pkt 11 RODO wskazuje, że jest to „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych". Definicja wskazuje, że zgoda nie może być przez administratora wymuszona, powinna być wyrażona wprost i musi określać osobę, która zgody udziela. Osoby te muszą wiedzieć także, komu udzielają zgody, jaki jest cel i zakres przetwarzania, a także przez jaki okres ich dane osobowe te będą przetwarzane.

»Obowiązkiem Administratora jest umożliwienie wycofanie zgody w tak samo łatwy sposób jak jej wyrażenie.«

Administrator musi pamiętać o prawie do wycofania zgody w dowolnym momencie przez osobę, która zgodę wyraziła. Ponadto administrator został zobowiązany do poinformowania osoby o tym prawie, zanim wyrazi ona zgodę.

Obowiązkiem Administratora jest także wdrożenie mechanizmów, które umożliwiają wycofanie zgody w tak samo łatwy sposób jak jej wyrażenie. Przykładem może być sytuacja, w której osoba wyraziła zgodę poprzez mechanizm zaimplementowany na stronie internetowej. W takim przypadku, na tejże stronie powinien istnieć analogiczny mechanizm do jej wycofania, a mechanizm taki powinien być łatwo dostępny i w żaden sposób nie powinien być ukryty.

Jak rozumieć i stosować podejście oparte na ryzyku?

Zgodnie z RODO, każdy podmiot musi samodzielnie oceniać ryzyko, jakie przetwarzanie danych osobowych może spowodować dla praw i wolności osób, których te dane dotyczą. To właśnie te wartości należy przede wszystkim brać pod uwagę.

Prezes Urzędu Ochrony Danych Osobowych (dawniej GIODO), przygotował dwuczęściowy poradnik.

W pierwszej części, zatytułowanej *Jak rozumieć podejście oparte na ryzyku według RODO?*, eksperci Urzędu Ochrony Danych Osobowych wyjaśniają istotę zasady podejścia opartego na ryzyku oraz wskazują, do czego zasada ta zobowiązuje podmioty stosujące przepisy ogólnego rozporządzenia o ochronie danych. Tłumaczą też, czym jest ryzyko naruszenia praw i wolności osób, których dane dotyczą. Podkreślają przy tym, że szacowanie ryzyka to proces ciągły, który powinien być przeprowadzany przy użyciu konkretnej metody, zapewniającej jednocześnie stosowanie jednolitych definicji i pojęć.

W drugiej części, zatytułowanej *Jak stosować podejście oparte na ryzyku?*, przedstawione zostały kolejne możliwe etapy działań podejmowanych w celu przeprowadzania ogólnej oceny ryzyka oraz szczegółowej oceny ryzyka, czyli tzw. oceny skutków dla ochrony danych.

Źródło: UODO

Pobierz poradniki

Aby je pobrać, zeskanuj wybrany kod lub kliknij na okładkę

RODO a anonimizacja i pseudonimizacja danych

Mimo, iż obowiązujące przepisy o ochronie danych osobowych stosujemy od maja 2018 roku, pojęcia anonimizacji i pseudonimizacji nadal sprawiają nie lada problem. Przyjrzyjmy się dokładnie ich znaczeniu.

Anonimizacja

Definicji anonimizacji danych osobowych na próżno szukać w RODO. Jednakże pojęcie to możemy znaleźć w ustawie o świadczeniu usług drogą elektroniczną. Oznacza ono nieodwracalne uniemożliwienie zidentyfikowania określonej osoby. Inaczej mówiąc, anonimizacja to trwałe usunięcie informacji wskazujących na osobę fizyczną, co skutkuje brakiem możliwości ustalenia personaliów osoby fizycznej, której pierwotnie dotyczyła informacja. Istotnym jest to, iż anonimizacja powoduje nieodwracalne usunięcie danych pozwalających na identyfikację danej osoby. Z uwagi na ten fakt, wobec zanonimizowanych danych nie stosuje się przepisów RODO.

Pseudonimizacja

Pseudonimizacja na gruncie RODO oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Równoległym warunkiem jest to, by takie dodatkowe informacje były przechowywane osobno i zostały objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej

Techniki depersonalizacji danych

Anonimizacja jest to proces, w którym dane osobowe są trwale i nieodwracalnie przekształcone. Technika ta uniemożliwia (w rozsądnym wymiarze czasowym i finansowym) przyporządkowanie informacji o określonej lub możliwej do zidentyfikowania osobie fizycznej.

Pseudonimizacja jest to odwracalny proces, polegający na zastąpieniu danej rzeczywistej nazwą przybraną, czyli nadanie jej tak zwanego pseudonimu. Pseudonimizacja utrudnia identyfikację, natomiast umożliwia przypisanie różnych czynności tej samej osobie (bez znajomości jej danych osobowych) oraz łączenie rożnych zbiorów danych między sobą. Pseudonimizacja skutecznie podwyższa bezpieczeństwo przetwarzania danych, ale nie jest równoznaczna anonimizacji, w związku z czym dane poddane pseudonimizacji dalej podlegają pełnej ochronie.

Źródło: Otwarte dane – standardy bezpieczeństwa, Ministerstwo Cyfryzacji, 2018

lub możliwej do zidentyfikowania osobie fizycznej. Innymi słowy, pseudonimizacja polega na zastępowaniu jednego atrybutu w zapisie innym atrybutem np. zmianie numeru PESEL na ciąg znaków, które można rozszyfrować wyłącznie na podstawie przechowywanych oddzielnie informacji – klucza. Takie działanie zwiększa poziom bezpieczeństwa danych. W związku z tym, że przy wykorzystaniu pseudonimizacji danych nadal istnieje prawdopodobieństwo pośredniego zidentyfikowania osoby fizycznej, zastosowanie tej metody nie będzie skutkowało anonimowym zbiorem danych.

W przeciwieństwie do anonimizacji, pseudonimizacja jest procesem całkowicie odwracalnym i dlatego też dane, które zostały w taki sposób zabezpieczone, w dalszym ciągu muszą być chronione zgodnie z wymogami RODO.

Grupa robocza art. 29 w opinii 05/2014 w sprawie technik anonimizacji wskazała, iż do najczęściej stosowanych technik pseudonimizacji należą m.in.:
– szyfrowanie z kluczem tajnym,
– funkcja skrótu, zwana także funkcją hashującą,
– tokenizacja.

Anonimizacja czy Pseudonimizacja? Co powinien wybrać Administrator Danych Osobowych?

Na pozór omawiane pojęcia są podobne, jednakże w rzeczywistości różnią się od siebie zasadniczo. Jedynym podobieństwem jest to, że obie techniki administratorzy danych mogą wykorzystywać w celu zabezpieczenia danych. Jednakże wybrane metody zabezpieczeń zależą od wielu czynników, w tym od przeprowadzonej analizy ryzyka, a także od celu, jaki administrator danych zamierza osiągnąć.

»Dane, które przeszły proces pseudonimizacji, można ponownie rozszyfrować na podstawie klucza.«

Każdorazowo administrator danych jest uprawniony i zobowiązany do wyboru takiego środka ochrony danych, który będzie zapewniał im należytą ochronę. W rezultacie tego, anonimizacja zdaje się być dobrym rozwiązaniem wtedy, gdy administrator chce lub jest zobowiązany do usunięcia danych osobowych. Pseudonimizacji może z kolei użyć w celu minimalizacji ryzyka utraty poufności danych – czyli jako mechanizm zabezpieczania danych przed określonymi zagrożeniami.

Podsumowując, administrator nie może stosować anonimizacji i pseudonimizacji w charakterze technik zamiennych, gdyż służą one osiąganiu odmiennych celów. ●

Trzy kluczowe dokumenty dla ochrony zdrowia

Aby je pobrać, zeskanuj poniższy kod lub kliknij na okładkę

Test równowagi, czyli określanie wagi interesów w przetwarzaniu danych

Administratorzy danych korzystający z prawnie uzasadnionego interesu jako przesłanki legalizującej przetwarzanie danych osobowych są zobligowani do przeprowadzenia testu równowagi.

Wymaganie przeprowadzenia testu wynika z art. 6 ust 1 lit f RODO o następującym brzmieniu: *„Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem."*

Prawodawca unijny przykłada szczególną uwagę do zapewnienia, aby przetwarzanie danych osobowych było realizowane w sposób zapewniający ochronę praw podstawowych, wolności i zasad uznanych w Karcie praw podstawowych Unii Europejskiej oraz do przepisów Konstytucji.

Wobec powyższego oczywistym jest, że posługiwanie się przesłanką „prawnie uzasadnionego interesu" dla legalizacji przetwarzania danych osobowych jest bardziej skomplikowane niż może się początkowo wydawać, gdyż wymaga od administratora przeprowadzenia analizy, która pozwoli na uzyskanie odpowiedzi na pytanie, czy skorzystanie z przesłanki prawnie uzasadnionego interesu jest możliwe.

Na czym polega test równowagi?

Test równowagi polega na wyważeniu interesu administratora realizowanego w związku z konkretną czynnością przetwarzania danych, a interesami lub podstawowymi prawami i wolnościami osób, których dane dotyczą. Wynik analizy powinien wskazać administratorowi, który z powyższych interesów ma charakter nadrzędny oraz w jaki sposób poprzez przetwarzanie danych w oparciu o tę przesłankę może naruszyć prawa i wolności podmiotów danych. W przypadku, gdy ważniejsze okażą się interesy lub podstawowe prawa i wolności osób, których dane dotyczą, administrator nie może skorzystać z przesłanki prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO) do przetwarzania danych osobowych w ramach analizowanej czynności.

Wskazówki jak przeprowadzić test równowagi?

Przeprowadzając test równowagi, warto oprzeć się o metodykę przeprowadzania testu tak, aby jego wyniki były mierzalne i powtarzane, szczególnie, jeżeli w naszej organizacji identyfikujemy wiele procesów przetwarzania danych osobowych opartych o przesłankę prawnie uzasadnionego interesu administratora.

Proponowane etapy przeprowadzenia testu równowagi*:

1. W pierwszej kolejności należy zidentyfikować prawnie uzasadnione inte-

resy administratora. Aby interes mógł być był uznany za prawnie uzasadniony, musi łącznie spełniać następujące warunki:
– być zgodny z prawem (UE oraz krajowym);
– być wystarczająco jasno wyrażony, tak aby pozwolić na przeprowadzenie testu równowagi względem interesów oraz podstawowych praw i wolności osoby, której dane dotyczą (musi być wystarczająco konkretny);
– stanowić rzeczywisty i obecny interes.

2. Następnie należy określić interesy lub podstawowe prawa i wolności podmiotów danych, które mogą zostać naruszone przetwarzaniem danych w oparciu o przesłankę prawnie uzasadnionych interesów.
3. Kolejnym krokiem jest zbadanie czy przetwarzanie danych w związku z daną czynnością jest niezbędne do realizacji prawnie uzasadnionego interesu administratora. Jeśli nie jest, wynik testu równowagi będzie zawsze negatywny, gdyż interesy podmiotu danych będą w takiej sytuacji miały charakter nadrzędny. Zawsze należy rozważyć czy nie istnieją inne, mniej inwazyjne środki do osiągnięcia określonego celu przetwarzania oraz służące interesowi administratora danych.
4. W przypadku pozytywnej odpowiedzi na powyższe pytania, należy określić, czyj interes w danej sytuacji ma charakter nadrzędny. W tym celu należy zwrócić uwagę na takie czynniki jak:
– charakter danych osobowych;
– status osoby (dziecko, pracownik) oraz administratora (na przykład, czy to jest organizacja biznesowa posiadająca dominującą pozycję na rynku);
– sposób, w jaki dane są przetwarzane (duża skala, profilowanie);
– kategorie podmiotów danych, sposoby przetwarzania danych, zastosowane środki bezpieczeństwa;
– należy zidentyfikować także podstawowe prawa i interesy osoby, której dane dotyczą, na które może być wywarty wpływ;
– należy rozważyć racjonalne oczekiwania osoby, której dane dotyczą;
– w końcu należy ocenić wpływ na osobę, której dane dotyczą, oraz porównać go z oczekiwanymi korzyściami z przetwarzania dla administratora danych.
5. Powyższa analiza powinna jasno określać, czyje interesy w danej sytuacji mają charakter nadrzędny – osoby, której dane dotyczą, czy administratora.
6. Zaleca się także udokumentowanie przeprowadzenia testu oraz jego wyników w celu zapewnienia rozliczalności wymaganej przez RODO.

Ustandaryzowanie powyższego procesu jest o tyle istotne, że w przypadku jednolitej metodyki i procedury przeprowadzania testu równowagi jego wyniki w podobnych sytuacjach będą porównywalne i mierzalne. Rozbieżność wyników takiego testu, która zależałaby od czynników ludzkich, stanowiłaby niepożądaną sytuację, która poprzez brak konsekwencji w przeprowadzaniu testu mogłaby narazić administratora danych na negatywny wynik kontroli UODO. ●

* Źródło: Opinia 6/2014 w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy artykułu 7 dyrektywy 95/46/WE

EROD wspiera w poprawnym reagowaniu na naruszenia ochrony danych

Nałożone w ostatnim czasie pieniężne kary administracyjne dowodzą, iż niemałym wyzwaniem dla administratorów danych osobowych (AOD) jest prawidłowe podejście do analizy i oceny naruszeń, które u nich wystąpiły.

Problemy występują mimo tego, iż Grupa Robocza Art. 29 opracowała reguły dotyczące zgłaszania naruszeń ochrony danych – wytyczne WP250. Na ten problem zwróciła także uwagę Europejska Rada Ochrony Danych (EROD), która jest niezależnym organem europejskim, działającym na rzecz spójnego stosowania zasad ochrony danych w całej Unii Europejskiej.

Na początku 2021 roku organ ten wydał wytyczne „EROD 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych". Dokument opisuje 18 naruszeń ochrony danych pogrupowanych w ramach sześciu rozdziałów:
– ataki typu ransomware,
– wycieki danych,
– błędy podczas wysyłki danych osobowych,
– kradzieże lub zagubienia urządzeń oraz dokumentów w formie papierowej,
– socjotechniki,
– zagrożenia pochodzące z wewnątrz organizacji.

W każdej z powyższych grup zostały opisane szczegółowe przykłady naruszeń i wskazówki, jak administratorzy danych powinni postąpić w przypadku, gdy stwierdzą takie naruszenie w stosunku do przetwarzanych danych osobowych.

Nie są to rzeczywiste przykłady, jednakże opierają się one na doświadczeniu organów nadzorczych w kwestiach powiadomień o wyciekach danych. Zanim przejdziemy do omówienia wybranych przykładów, należy wyraźnie wskazać, iż jednym z najważniejszych obowiązków AOD jest ocena zidentyfikowanych zagrożeń wobec praw i wolności osób,

których dane dotyczą oraz wdrożenie odpowiednich środków technicznych i organizacyjnych w celu przeciwdziałania zaistniałym zagrożeniom. W związku z tym RODO wymaga aby administrator:
– udokumentował wszelkie naruszenia ochrony danych osobowych, w tym okoliczności w jakich naruszenie wystąpiło, jego skutki oraz podjęte działania naprawcze;
– powiadomił organ nadzorczy o naruszeniu danych osobowych, chyba że jest mało prawdopodobne, aby naruszenie danych powodowało zagrożenie dla praw i wolności osoby fizycznej;
– zawiadomił osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych, gdy istnieje prawdopodobieństwo, że naruszenie danych osobowych spowoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych.

Pierwszą grupą zagrożeń, na jaką zwróciło uwagę EROD, są spędzające sen z powiek AOD ataki typu ransomware, polegające na szyfrowaniu danych w zbiorach administratora. Wytyczna zawiera opis kilku przykładowych naruszeń oraz podpowiedzi, jak należy postąpić w takich okolicznościach.

Przykład: Atak typu ransomware, administrator posiada odtwarzalną kopię zapasową, nie miał miejsca wyciek danych.

Pierwszym przykładem jest naruszenie mogące mieć miejsce w małej firmie produkcyjnej, która stała się celem ataku typu ransomware. Należy jednak zaznaczyć, że administrator gromadził dane w postaci zaszyfrowanej, a do ich zaszyfrowania zostały zastosowane najnowsze techniki kryptograficzne. Klucz deszyfrujący nie został naruszony podczas ataku, a także atakujący nie uzyskał do niego dostępu. W związku z tym, atakujący posiadał dostęp wyłącznie do danych zaszyfrowanych, bez możliwości ich odszyfrowania. Atakujący nie był w stanie również uzyskać dostępu do innych zasobów ani systemów administratora. Po przeprowadzaniu profesjonalnej analizy zdarzenia stwierdzono, że sprawcy włamania wyłącznie zaszyfrowali część danych. Informacje w logach nie wykazały wycieku danych. Administrator posiadał kopię zapasową zaszyfrowanych przez atakujących danych i dzięki temu dane zostały przywrócone. Po kilku godzinach procesy działały w sposób niezakłócony.

»Jak powinien zareagować administrator danych osobowych, gdy w szpitalu miał miejsce atak typu ransomware.«

Jak powinien postąpić administrator danych? Rekomenduje się aby naruszenie zostało udokumentowane w wewnętrznym rejestrze naruszeń.

Przykład: Atak typu ransomware, który miał miejsce w szpitalu, administrator posiada odtwarzalną kopię zapasową, nie miał miejsca wyciek danych.

Tym razem atak ma miejsce w szpitalu, w którym znaczna część danych gromadzonych w systemach została zaszyfrowana przez atakującego. Szpital korzysta z wiedzy zewnętrznej firmy zajmującej się cyberbezpieczeństwem, aby monitorować swoją sieć. Dostępne są dzienniki śledzące wszystkie przepływy danych. Po przeanalizowaniu logów ustalono, że sprawca jedynie zaszyfrował dane i nie doszło do wycieku. Dzienniki nie pokazują żadnego przepływu danych na zewnątrz w okresie ataku. Dane osobowe, których dotyczy naruszenie, dotyczą pracowników i pacjentów. Kopie zapasowe były dostępne w formie elektronicznej. Większość danych została przywrócona, ale operacja ta trwała 2 dni robocze i doprowadziła do poważnych opóźnień w leczeniu pacjentów wraz z odwołaniem lub przełożeniem operacji, tak więc sytuacja doprowadziła do obniżenia poziomu usług z powodu niedostępności systemów.

Jak powinien postąpić administrator danych? Z uwagi na wysokie ryzyko naruszenia praw i wolności osób fizycznych należy udokumentować naruszenie w wewnętrznym rejestrze, zgłosić naruszenie organowi nadzorczemu oraz zawiadomić osoby, których dane dotyczą.

Powyższe przykłady przedstawiają podobne sytuacje, lecz konsekwencje dla osób, których dane dotyczą, są odmienne – dlatego tak ważna jest wnikliwa analiza zdarzenia i jego skutków. EROD nie zostawia jednak administratora danych bez wskazówek, po jakie środki zaradcze sięgnąć, aby przeciwdziałać tego typu atakom. Przykładami zaproponowanymi przez EROD są:
– regularne aktualizacje oprogramowania;
– istnienie aktualnej, bezpiecznej i przetestowanej procedury tworzenia kopii zapasowych;
– posiadanie aktualnego oraz kompleksowego oprogramowania antywirusowego;
– posiadanie aktualnego, odpowiednio skonfigurowanego oraz efektywnego firewall'a oraz systemów wykrywania włamań;
– cykliczne szkolenia pracowników w zakresie metod rozpoznawania i zapobiegania atakom informatycznym;
– silne metody szyfrowania i uwierzytelniania, w szczególności w przypadku dostępu administracyjnego w tym dwustopniowe uwierzytelnianie;
– regularnie przeprowadzane audyty podatności oraz testy penetracyjne;
– posiadanie zespołów reagowania na incydenty bezpieczeństwa;
– oceniając zabezpieczenia należy zawsze dokonać analizy ryzyka.

Należy również pamiętać, iż każda czynność przetwarzania jest inna, dlatego administratorzy powinni podjąć decyzję, które środki najlepiej pasują do danej sytuacji.

Przedstawione powyżej przykłady to jedynie dwa z 18 zdarzeń. Po więcej odsyłamy do dokumentu EROD 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych, dostępnego w języku angielskim na stronie www.uodo.gov.pl.

Wnioski płynące z rocznego sprawozdania z działalności Prezesa UODO

Do końca sierpnia każdego roku Prezes Urzędu Ochrony Danych Osobowych zobowiązany jest do przygotowania sprawozdania ze swojej rocznej działalności. Sprawozdanie nie tylko dostarcza nam informacji statystycznych dotyczących bieżących działań Urzędu, ale także wybrane stanowiska UODO w zakresie stosowania obowiązujących przepisów o ochronie danych osobowych i najczęściej zgłaszane naruszenia.

Niniejszy artykuł ma na celu zapoznanie czytelnika z najistotniejszymi informacjami zamieszczonymi w sprawozdaniu, a także wnioskami, jakie niesie dla Administratorów Danych Osobowych opublikowany przez UODO raport.

Na początek garść liczb, które jednoznacznie wskazują, że organ nie tylko wywiązuje się z obowiązków nakładanych na niego przez RODO, ale także systematycznie zwiększa swoją aktywność. W 2020 roku UODO zanotował 7507 naruszeń, czyli ponad trzykrotnie więcej niż w 2018 roku. Zanotowano 6442 skarg osób, których dane dotyczą (wzrost o 15%). W tym czasie UODO wydał 1866 decyzji administracyjnych, znacznie więcej niż w poprzednich latach. Choć na początku działalności, w 2018 roku, UODO nie nałożył żadnej kary pieniężnej, to w 2019 roku było ich już 8, a w 2020 roku – 11.

Dziwić może znacznie mniejsza liczba przeprowadzonych kontroli. Powodem tego mogą być zmiany w strukturze organizacyjnej Urzędu, które były konsekwencją doświadczeń wynikających z funkcjonowania w latach 2018 – 2019 zespołów tematycznych. Ten kierunek został utrzymany i w efekcie w Urzędzie Ochrony Danych Osobowych podjęto decyzję o stworzeniu Departamentu Skarg. W jego ramach utworzono cztery wydziały tematyczne: Wydział ds. Sektora Publicznego, Wydział ds. Sektora Prywatnego, Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa, Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji.

»W 2020 r. do UODO wpłynęło 926 skarg na podmioty sektora zdrowia, zatrudnienia i szkolnictwa.«

Głównym zadaniem Departamentu Skarg i wchodzących w jego skład Wydziałów jest rozpatrywanie zgłaszanych skarg na nieprawidłowości w procesie przetwarzania danych osobowych. Utworzenie wydziału ds. Sektora Zdrowia, Zatrudniania i Szkolnictwa wskazuje, że skarg, w tym sektorze jest coraz więcej, co potwierdzą dane opublikowane w sprawozdaniu.

Liczba skarg, które w analizowanym okresie sprawozdawczym 2020 wpłynęły do UODO, z podziałem na sektory, przedstawia się następująco:
- 1303 skargi na podmioty sektora publicznego,
- 2519 skarg na podmioty sektora prywatnego,
- 926 skarg na podmioty sektora zdrowia, zatrudnienia i szkolnictwa,
- 1694 skargi na podmioty sektora finansowego, ubezpieczeń i telekomunikacji.

Naruszenia a COVID-19

Organ nadzorczy opublikował w sprawozdaniu, że w 2020 r. pojawiało się wiele naruszeń wynikających z działań podejmowanych w związku z zagrożeniem epidemicznym. Jak sygnalizuje UODO, w dużej części były to działania polegające na stosowaniu nowych środków, mających na celu ochronę zdrowia osób, których dane dotyczyły, a które wcześniej nie były poddawane analizie pod kątem wystąpienia możliwych zagrożeń i podatności. UODO wskazało, że do naruszeń dochodziło również w podmiotach, które przed 2020 r. posiadały szczegółowo opracowane procedury dot. przetwarzania danych osobowych, a które w czasie niemożliwej do przewidzenia pandemii nie sprawdziły się. Jako przykłady takich sytuacji UODO wskazał:
- nieprawidłowości w zakresie weryfikacji tożsamości osób, którym wydawana była dokumentacja medyczna;
- ataki złośliwym oprogramowaniem typu ransomware w związku ze wzrostem e-rozwiązań oferowanych przez podmioty medyczne oraz prowadzeniem dokumentacji w formie elektronicznej;
- ujawnianie danych osób objętych kwarantanną przez podmioty, których zadaniem było przeciwdziałanie rozszerzaniu się epidemii.

Najczęściej zgłaszane oraz typowe naruszenia w 2020 r.

Poniżej przedstawiona została lista naruszeń, które były najczęściej zgłaszane w 2020 r. do UODO. Każdy Administrator Danych Osobowych powinien przeanalizować ją dokładnie i podjąć środki minimalizujące ryzyko ich wystąpienia w swoich organizacjach:
- wysyłanie korespondencji (zarówno w formie tradycyjnej, jak i elektronicznej) zawierającej dane osobowe do niewłaściwego odbiorcy;
- ujawnianie danych niewłaściwej osobie, np. poprzez wydanie dokumentów osobie, dla której nie były przeznaczone;
- nieuprawnione uzyskanie dostępu do informacji, czego przyczyną były m.in.:
  - błędy programistyczne, ujawniające się po wprowadzeniu aktualizacji oprogramowania;
  - brak wewnętrznych testów bezpieczeństwa, które mogły wykazać podatność systemu;
  - nieprawidłowo nadane uprawnienia w systemach informatycznych, czego skutkiem było zapoznanie się z danymi osobowymi przez osoby do tego nieuprawnione;
- utrata korespondencji papierowej przez operatora pocztowego lub otwarcie korespondencji przed zwróceniem do nadawcy;
- zagubienie, kradzież dokumentacji papierowej (zawierającej dane osobowe) lub pozostawienie jej w niezabezpieczonym miejscu, w szczególności wynoszenie przez pracowników dokumentów poza zakład pracy i pozostawianie jej w miejscach publicznych;
- niezamierzona publikacja lub nieprawidłowa anonimizacja danych w dokumencie – zdarzenia te polegały na publikacji danych osobowych na stronie internetowej administratora oraz udostępnieniu w trybie dostępu do informacji publicznej;
- zgubienie lub kradzież nośnika danych/urządzenia umożliwiającego dostęp do danych tego typu zdarzenia będące najczęściej wynikiem kradzieży komputera przenośnego lub zgubienia niezaszyfrowanego elektronicznego nośnika danych;
- złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych oraz nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń. Do tego typu naruszeń najczęściej dochodziło w wyniku wykorzystania wyspecjalizowanych umiejętności osób prowadzących takie ataki oraz wykorzystania podatności atakowanych systemów. Niejednokrotnie przyczyniali się do tego sami administratorzy, wykorzystując do przetwarzania danych nieaktualne oprogramowanie. ●

Sprawozdanie z działalności UODO za latach 2018–2020

	2018 r.	2019 r.	2020 r.
Skargi osób, których dane dotyczą	5565	9304	6442
Zgłoszone naruszenia	2446	6039	7507
Liczby przeprowadzonych kontroli	72	98	12
Liczba pracowników	235	246	277 (na dzień 31.12.2020 r.)
Wydane decyzje administracyjne	527	1369	1866
Kary pieniężne	0	8	11
Wydatki UODO	25 681 000 zł	31 390 000 zł	34 898 000 zł

Źródło: UODO

85 tysięcy zł za naruszenie danych osobowych

Prezes UODO nałożył pierwszą karę na podmiot z sektora ochrony zdrowia. Powodem był brak poinformowania pacjentów o wycieku danych osobowych.

Decyzja o nałożeniu przez Prezesa UODO pierwszej w Polsce administracyjnej kary pieniężnej na podmiot medyczny nie odbiła się szerokim echem. Prawdopodobną przyczyną było to, że w ostateczności kara została nałożona za brak współpracy z UODO, a nie za sam wyciek.

Sprawa wygląda następująco. Do Urzędu Ochrony Danych Osobowych wpłynęło zgłoszenie naruszenia ochrony danych osobowych. Z jego treści wynikało, iż doszło do nieuprawnionego skopiowania danych osobowych stu pacjentów z systemu podmiotu medycznego przez byłego pracownika w celu ich wykorzystania do marketingu własnych usług. Jednocześnie wskazane zostało, że naruszenie dotyczyło następujących kategorii danych osobowych pacjentów: numeru PESEL, imion i nazwisk, imion rodziców, daty urodzenia, adresu zamieszkania lub pobytu, numeru telefonu.

Podmiot medyczny nie powiadomił jednak osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, i to pomimo, że ocenił ryzyko naruszenia praw i wolności osób fizycznych jako wysokie. W związku z powyższym, Prezes UODO wezwał podmiot do niezwłocznego zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych oraz przekazania im zaleceń odnośnie zminimalizowania potencjalnych negatywnych skutków zaistniałego naruszenia.

W kolejnych wyjaśnieniach podmiotu zawarto informacje o braku możliwości zidentyfikowania osób, których dotyczyło naruszenie. Co więcej – dowiadujemy się także, że pracownikiem, który skopiował dane pacjentów, był lekarz zatrudniony wówczas w podmiocie medycznym. Pomimo działań realizowanych przez podmiot, których celem miało być prawidłowe zawiadomienie o zaistniałym naruszeniu osób, których dane dotyczą, Prezes UODO ocenił, iż nie przedstawił on wystarczających dowodów na wykonanie obowiązku zawiadomienia, o którym mowa w art. 34 ust. 1 i 2 RODO.

Jak czytamy dalej w decyzji Prezesa UODO, właściwe wywiązanie się z obo-

»Podmiot kary mógł uniknąć, gdyby wywiązał się z zaleceń UODO.«

wiązku zawiadomienia osób poszkodowanych pozwoliłoby zrozumieć osobom, których dane dotyczą, na czym polegało naruszenie ochrony ich danych osobowych, poznać możliwe konsekwencje takiego zdarzenia oraz podjąć działania w celu zminimalizowania ewentualnych negatywnych skutków.

Podmiot medyczny mógł uniknąć nałożonej kary. Wystarczyło wywiązać się z zaleceń Prezesa UODO. Zwłaszcza, że jak wynika z decyzji, urzędnik UODO przekazywał podmiotowi wskazówki jak prawidłowo należy zawiadomić osoby, których dotyczyło naruszenie. Co więcej, jest to kolejny przykład na to, że nie można lekceważyć naruszeń ochrony danych osobowych, których w pewnych okolicznościach, nie da się uniknąć.

W każdym przypadku warto współpracować z organem nadzorczym, przestrzegać otrzymanych wskazówek i zaleceń, a przede wszystkim podnosić wiedzę z zakresu ochrony danych osobowych oraz bezpieczeństwa informacji wśród personelu. Wysokość nałożonej kary (85 588 złotych) wskazuje, że organ nadzorczy z całą pewnością zastosował proporcjonalną, skuteczną i odstraszającą karę – zgodnie z art. 83 RODO, właśnie takimi cechami powinna się charakteryzować nałożona administracyjna kara pieniężna.

To kolejna kara Prezesa UODO za brak współpracy. Przypomnijmy, nie tak dawno, bo w czerwcu br., opublikowana została decyzja nakładająca karę w wysokości 22 tys. za brak współpracy z organem nadzorczym. W tym przypadku podmiot, w stosunku do którego wpłynęła skarga za nieprawidłowości w procesie przetwarzania danych, nie udzielił żadnej odpowiedzi na pisma UODO. ●

ANEKS

Etapy wdrażania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w podmiocie przetwarzającym dokumentację medyczną

Stworzenie planu postępowania z ryzykiem

Jeżeli zagrożenia zostały zidentyfikowane na podstawie analizy ryzyka, to ryzyko powinno być zbadane i albo zaakceptowane przez kierownictwo wyższego szczebla lub zredukowane, jeżeli ryzyko to jest uważane za niedopuszczalne. Plan redukcji ryzyka precyzuje działania, które muszą być przeprowadzone, aby zmniejszyć poziom niedopuszczalnego ryzyka. Obejmuje on plan wdrażania kontroli bezpieczeństwa wybranych zagrożeń, mających na celu ich redukcję lub akceptację. SZBI jest odpowiedzialny za zapewnienie, że plan ten jest przeprowadzany. Najlepiej, plan redukcji ryzyka będą obejmować harmonogramy, priorytety i szczegółowe plany pracy, a także przydzielenie odpowiedzialności za prowadzenia kontroli bezpieczeństwa. W opiece zdrowotnej, zatwierdzanie takich planów jest kluczowym etapem związanym z postępowaniem z ryzykiem.

Przydzielanie zasobów

Istotną rolą zarządzania jest zapewnienie niezbędnych zasobów (ludzkich, systemowych i finansowych) w celu zapewnienia bezpieczeństwa zasobów informacyjnych dot. obszaru zdrowia.

Wybór i realizacja sposobu kontroli bezpieczeństwa

Ocena każdego z obszarów kontroli zabezpieczeń wynika bezpośrednio z normy ISO/IEC 27002 gdzie zawarte są porady i wskazówki dotyczące kontroli bezpieczeństwa w środowisku opieki zdrowotnej.

Kształcenie i wychowanie

Bardzo ważnym jest, aby opracowano i realizowano wymagania dotyczące szkoleń i edukacji dla wszystkich pracowników, wykonawców, służby zdrowia i innych, którzy mają dostęp do systemów informatycznych przetwarzających dokumentację medyczną i osobiste Informacje na temat zdrowia.

Zarządzanie SZBI

Właściwa eksploatacja SZBI jest niezbędna, jeśli poufność, integralność i dostępność systemów informatycznych i informacyjnych systemów zdrowia ma być utrzymana.

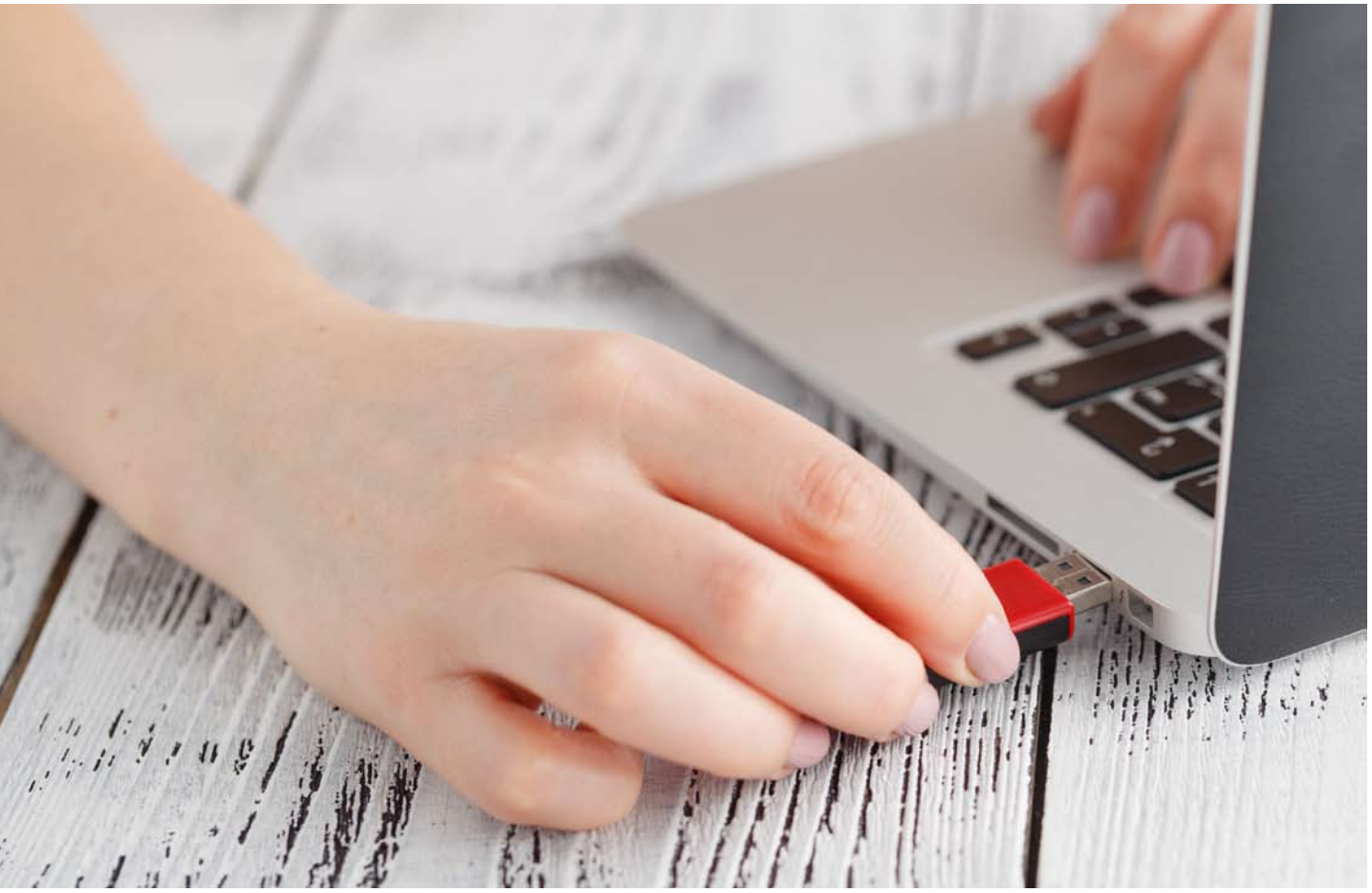
Zarządzanie zasobami

Efektywna ochrona informacji może być kosztowna, a kompetentne zasoby ludzkie ograniczone. Skuteczne określenie priorytetów przez najwyższy szczebel kierownictwa oraz zaangażowanie niezbędnych zasobów ludzkich ma na celu zapewnienie bieżącej działalności.

Zarządzanie incydentami bezpieczeństwa

W celu zminimalizowania skutków incydentu bezpieczeństwa, ważne jest, że incydent ma być wykryty odpowiednio i że należy podjąć działania naprawcze. Procedury postępowania w przypadku wystąpienia incydentów związanych z naruszeniem bezpieczeństwa informacji muszą być poddawane regularnym przeglądom. Szczególnie ważne jest określenie obowiązków i sposobu działania w początkowej fazie reakcji, jako że zdarzenia rozwijają się szybko i krytyczny charakter systemów informacji zdrowotnej pozostawia niewiele czasu na reakcję. Przejrzyste procedury raportowania o zdarzeniach bezpieczeństwa są bardzo istotne, ponieważ regulują sposoby informowania o zdarzeniach i ich skutkach.

Źródło: Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej



Niezabezpieczony pendrive skutkuje karą UODO

W ramach cyklicznego informowania czytelników czasopisma OSOZ o kolejnych decyzjach wydawanych przez Prezesa UODO, niniejszy artykuł zostanie poświęcony analizie decyzji dotyczącej braku zastosowania odpowiednich zabezpieczeń nośników służących do gromadzenia danych osobowych.

Do prezesa UODO wpłynęło zgłoszenie naruszenia ochrony danych osobowych, którego nadawcą był prezes jednego z Sądów Rejonowych. Zgłoszenie zawierało informacje o naruszeniu ochrony danych osobowych czterystu osób podlegających nadzorowi kuratorskiemu i objętych wywiadem środowiskowym przez kuratora sądowego.

Zakres danych podlegający naruszaniu to imiona i nazwiska, daty urodzenia, adresy zamieszkania lub pobytu, numery PESEL, serie i numery dowodów osobistych, numery telefonów, dane dotyczące zarobków lub posiadanego majątku, dane dotyczące zdrowia oraz wyroków skazujących. Incydent stanowiący przedmiot zgłoszenia polegał na zagubieniu przez kuratora sądowego nieszyfrowanej, przenośnej pamięci zewnętrznej typu pendrive. Z uwagi na zakres ujawnionych danych osobowych, naruszenie spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych, dlatego też administrator, zgodnie z art. 34 RODO, opublikował na stronie internetowej Sądu Rejonowego komunikat o naruszeniu.

W toku postępowania, administrator danych osobowych wykazał, iż wdrożył system ochrony danych w postaci zasad

przetwarzania danych osobowych. Dokumentacja ta była na bieżąco aktualizowana i audytowana przez powołanego do tego celu inspektora ochrony danych. Ponadto administrator zapewnił, że podejmował działania w postaci szkoleń z zakresu ochrony danych osobowych, jednakże, zgodnie z obowiązującymi u administratora dokumentami, obowiązek zabezpieczenia nośników spoczywał na użytkownikach nośników.

UODO uznało, iż takie podejście jest niewłaściwe i skutkowało naruszeniem zasad poufności i integralności danych osobowych poprzez wydanie do użytku służbowego kuratorom sądowym niezabezpieczonej przenośnej pamięci zewnętrznej. Co więcej, zobowiązał ich do wdrożenia zabezpieczeń tego narzędzia we własnym zakresie.

Wnioski dla przedsiębiorców, w tym podmiotów wykonujących działalność leczniczą:
– Omówiona wyżej decyzja potwierdza, że to administrator danych osobowych, a nie użytkownik odpowiada za wdrożenie środków technicznych i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa przetwarzanych danych osobowych;
– Niewystarczające jest polecenie zabezpieczenia nośników pracownikom i pozostawienie im dowolności w wyborze zabezpieczeń odpowiednich do istniejących ryzyk;
– Nie oznacza to, że w każdym przypadku Administrator sam powinien zabezpieczać nośniki zgodnie z przeprowadzoną analizą ryzyk, natomiast powinien zlecić wykonanie określonych czynności wykwalifikowanemu pracownikowi lub zewnętrznemu podmiotowi;
– Działania Administratora powinny zostać przez niego zaplanowane, kontrolowane i powinny wynikać z obowiązującej w organizacji dokumentacji ochrony danych osobowych;
– UODO wskazuje, iż poza dokumentacją i wdrożeniem odpowiednich zabezpieczeń konieczne jest przeprowadzenie szkoleń z zakresu ochrony danych osobowych. Należy jednak pamiętać, że szkolenia są wyłącznie jednym z elementów poprawnie działającego systemu ochrony danych osobowych i na pewno wpływają na poziom bezpieczeństwa, lecz nie zastępują wdrożenia zabezpieczeń, gdyż wektorem ataku nie zawsze jest nieświadomy pracownik. ●

ANEKS

Incydenty bezpieczeństwa

W ramach zarządzania incydentami naruszenia bezpieczeństwa informacji powinny zostać sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn. Powinny zostać opracowane regulacje wewnętrzne opisujące zasady postępowania w przypadkach wystąpień incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego, czyli m.in. awarii i przeciążeń systemów informatycznych, utraty urządzeń lub danych, błędów ludzkich skutkujących zagrożeniem dla bezpieczeństwa środowiska teleinformatycznego, naruszeń lub prób naruszeń zabezpieczeń, niekontrolowanych zmian w systemach itp.

Zakres i poziom szczegółowości powyższych regulacji powinny być adekwatne do skali i specyfiki przetwarzania informacji oraz poziomu złożoności jego środowiska teleinformatycznego. Zasady postępowania z incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego powinny w szczególności określać:
– metody i zakres zbierania informacji o incydentach,
– zakresy odpowiedzialności w obszarze zarządzania incydentami,
– sposób przeprowadzania analiz wpływu incydentów na środowisko teleinformatyczne, w tym jego bezpieczeństwo,
– zasady kategoryzacji i priorytetyzacji incydentów, uwzględniające klasyfikację informacji i systemów informatycznych związanych z danym incydentem,
– zasady wykrywania zależności pomiędzy incydentami (przykładem tego rodzaju zależności jest atak typu „Denial-of-Service" uniemożliwiający szybką identyfikację innego incydentu lub usunięcie jego przyczyn),
– zasady komunikacji, obejmujące zarówno pracowników, jak i zewnętrznych dostawców usług oraz – w przypadku istotnego narażenia na skutki danego incydentu – również innych stron trzecich, zapewniające odpowiednio szybkie powiadamianie zainteresowanych stron i podejmowanie działań, adekwatnie do poziomu istotności incydentu,
– zasady gromadzenia i zabezpieczania dowodów związanych z incydentami, które będą mogły zostać wykorzystane w ewentualnych postępowaniach sądowych (w szczególności minimalizujące ryzyko utraty takich dowodów lub ich odrzucenia ze względu na niewłaściwe zabezpieczenie danych),
– zasady dotyczące podejmowania działań naprawczych i zapobiegawczych, obejmujące w szczególności przypisanie osób odpowiedzialnych za realizację tych działań oraz monitorowanie stanu ich realizacji.

W celu m.in. umożliwienia podejmowania działań zapobiegawczych w odniesieniu do identyfikowanych problemów, powinien być prowadzony rejestr incydentów naruszenia bezpieczeństwa informacji, w którym przechowywane powinny być w szczególności informacje dotyczące:
– daty wystąpienia i identyfikacji incydentu,
– przyczyn zajścia incydentu,
– przebiegu incydentu,
– skutków incydentu,
– podjętych działań naprawczych. ●

Źródło: Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej

KAMSOFT S.A.

Zadbaj o **bezpieczeństwo** danych osobowych w Twojej placówce medycznej z KS-BDO RODO!

- **Wsparcie** w przeprowadzeniu analizy ryzyka
- **Ankieta** umożliwiająca ocenę indywidualnej sytuacji podmiotu w obszarze przetwarzania danych osobowych
- **Wzorce** dokumentów wykorzystywanych w procesach przetwarzania danych osobowych
- **Wskaźniki** poziomu wdrożenia rekomendowanych zabezpieczeń
- Wbudowane **mechanizmy aktualizacji** dokumentacji w obszarze wynikającym ze zmian personalnych
- Wbudowane **rejestry** pozwalające dokumentować czynności związane z przetwarzaniem danych

Rozwiązanie KS-BDO RODO współpracuje z systemami produkcji KAMSOFT: KS-AOW, KS-SOMED, KS-PPS.

kontakt@osoz.pl | tel. (+48) 32 209 07 05

kamsoft.pl/KS-BDO-RODO

Wpływ pandemii COVID-19 na cyberbezpieczeństwo

Wybuch pandemii COVID-19 wiązał się z wieloma wyzwaniami dla pracodawców. Jednym z nich była organizacja pracy zdalnej, co nie pozostało bez wpływu na kwestię bezpieczeństwa danych. O sposobach i poradach dotyczących zapewniania wysokiego poziomu bezpieczeństwa podczas pracy zdalnej pisaliśmy w numerze 6/2020. Dziś podsumowujemy, jaki wpływ na bezpieczeństwo miała decyzja o zdalnej pracy i czy pracodawcy ograniczyli ryzyka z nią związane.

Publikowany co roku przez IBM raport „Cost of A Data Breach" nie pozostawia złudzeń, że zaistniała sytuacja epidemiczna miała ogromny wpływ na stan bezpieczeństwa danych. Prawie 80% badanych organizacji jest przekonana, że pandemia wpłynie na pogorszenie stanu cyberbezpieczeństwa. Wśród ponad 500 badanych organizacji z kilkunastu krajów na świecie, które padły ofiarą cyberprzestępców, średnia wielkość szkody wyrządzona tymi atakami wynosi prawie 3,9 mln dolarów. Jednakże należy podkreślić, że raport publikowany jest za okres tylko częściowo obejmujący czas pandemii COVID-19. Mimo to, autorzy raportu szacują, że sama praca zdalna spowodowała wzrost wysokości średniej szkody o 137 tys. dolarów.

Dlaczego zmiana trybu pracy na zdalny ma tak znaczny wpływ na stan bezpieczeństwa organizacji? Jak pokazuje raport Komisji Europejskiej „Cyber security: What Europeans think" z początku 2020 roku, blisko połowa Europejczyków nie jest świadoma istnienia cyberzagrożeń. I choć sytuacja uległa poprawie w ostatnich latach, to tempo tych zmian jest niewystarczające biorąc pod uwagę dynamiczny wzrost działań cyberprzestępców.

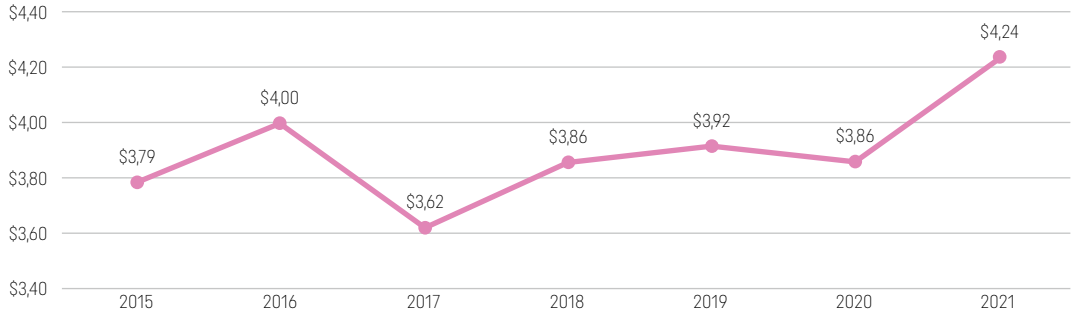
Niski poziom świadomości istnienia zagrożeń, w połączeniu ze wzrostem częstotliwości prób ataków, w szczególno-

ści ataków typu phishing i ransomware, sprawia, że wiele organizacji jest obecnie dużo bardziej podatnych na atak niż przed pandemią. Takiemu stanowi sprzyja także korzystanie przez pracowników ze sprzętu prywatnego np. domowych routerów wi-fi, bardzo często z fabrycznymi ustawieniami, wykonywanie na jednym komputerze zadań służbowych i prywatnych ze względu na brak dostępności sprzętu w organizacjach oraz u dostawców, wysoka podatność na działania socjotechniczne spowodowane obawami o zdrowie swoje i najbliższych. Wymienione czynniki sprzyjają tym wszystkim, którzy zobaczyli szansę na zysk płynący z działalności cyberprzestępczej.

Warto także podkreślić, że skutkiem pandemii dla wielu organizacji było zagrożenie dla stabilności finansowej, a co za tym idzie brak funduszy kierowanych na walkę z nowo pojawiającymi się zagrożeniami cyberbezpieczeńsywa. Niestety brakuje analizy, jaki wpływ na działalność w zmienionych warunkach mogą mieć nowe zagrożenia. Nierzadko powodowały one kolejne straty finansowe dla organizacji, co potwierdzają badania przywoływanego wyżej raportu – 40% szkód wynikających z ataków hackerskich stanowią utracone przychody przedsiębiorstwa. ●

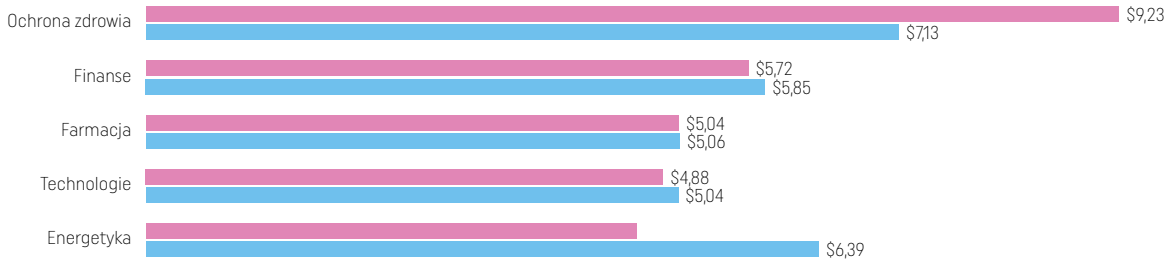
»Średni koszt wycieku danych w 2020 roku wyniósł 4,24 mln USD.«

Średni całkowity koszt naruszenia bezpieczeństwa danych w mln USD



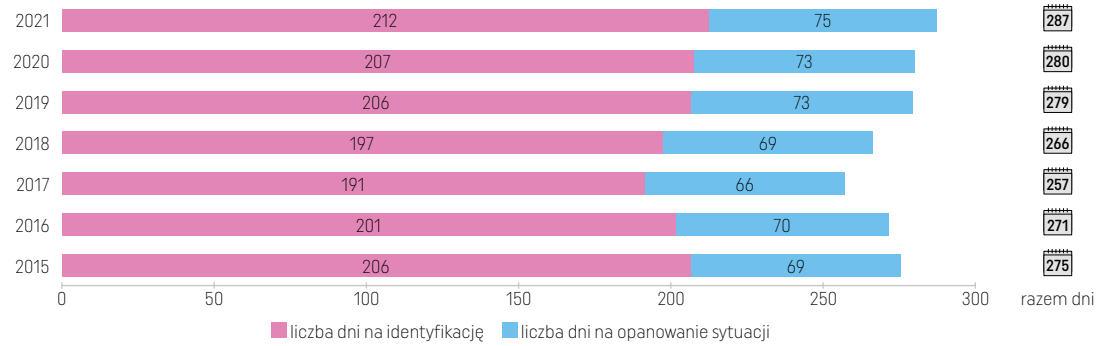
Źródło: IBM

Średni całkowity koszt naruszenia bezpieczeństwa danych w zależności od branży (w mln USD)

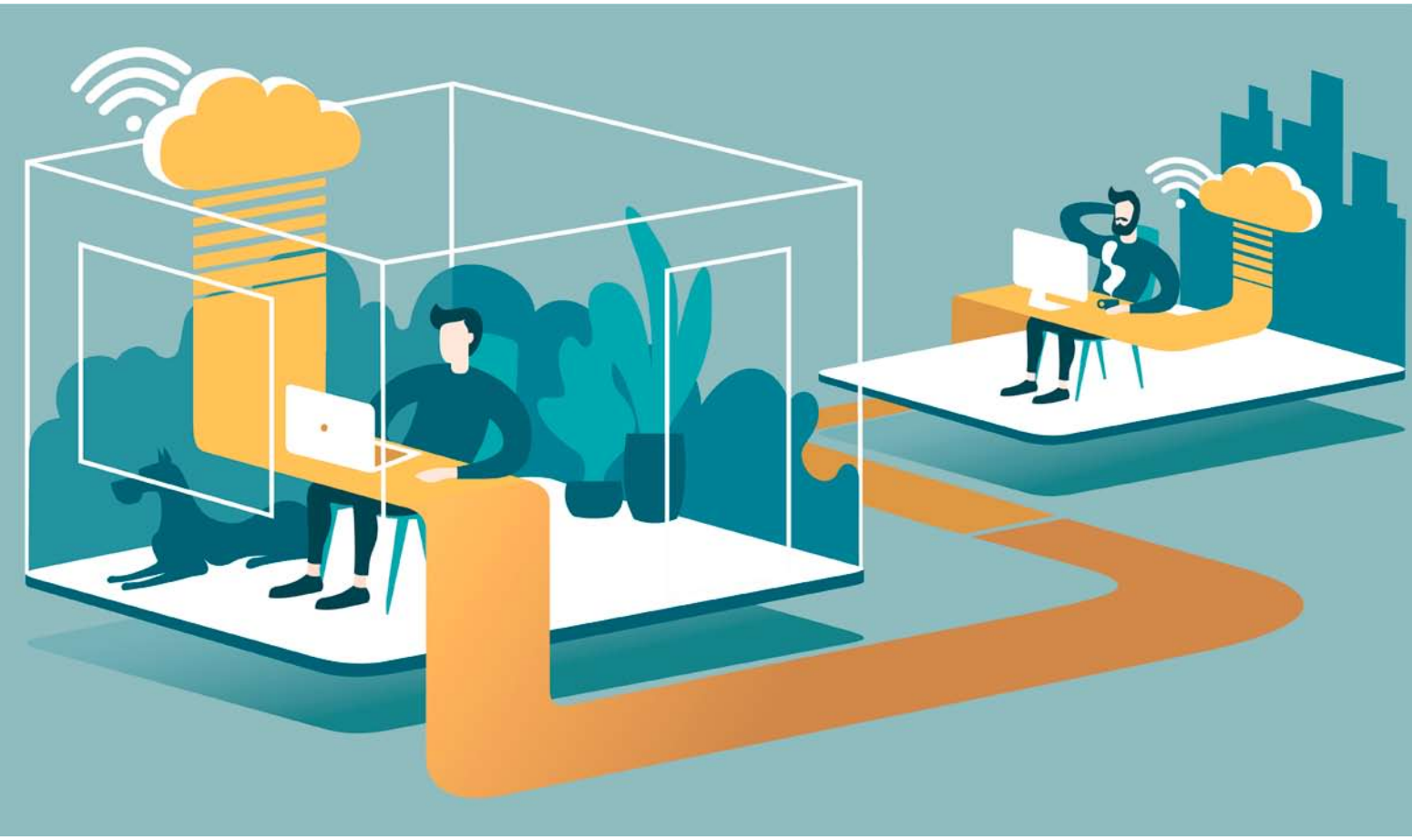


Źródło: IBM

Średni czas identyfikacji i opanowania naruszenia bezpieczeństwa danych (w dniach)



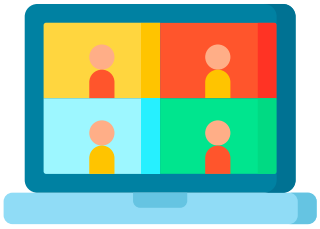
Źródło: IBM



Ochrona danych osobowych podczas pracy zdalnej

W jaki sposób zagwarantować bezpieczeństwo danych, gdy dom zamienia się w biuro?

W obliczu zaistniałej sytuacji epidemicznej wiele firm, gdy tylko to możliwe, decyduje się na zmianę organizacji pracy i rekomenduje pracownikom pracę zdalną. Pomimo wielu zalet tego podejścia, pracodawcy zastanawiają się jak postępować podczas pracy zdalnej, aby nie naruszyć przepisów o ochronie danych oraz jak zapewnić bezpieczeństwo danych przetwarzanych przez pracowników. Praca zdalna to wiele szans, a jedną z nich jest ograniczenie rozprzestrzeniania się COVID-19. Jednakże to też ryzyka, na które nie każdy pracodawca zdążył się przygotować. Poniżej przedstawiam porady dotyczące bezpieczeństwa danych osobowych podczas pracy poza biurem.



Wideokonferencja

- Do zainstalowania aplikacji służącej do przeprowadzania wideokonferencji na komputerze użyj oficjalnej strony dostawcy aplikacji, z której chcesz korzystać. W przypadku urządzeń mobilnych, wybierz oficjalny sklep.
- Przed instalacją zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego chcesz skorzystać.

»Pomimo wielu zalet pracy zdalnej, pracodawcy zastanawiają się, jak postępować, aby nie naruszyć przepisów o ochronie danych.«

- Zweryfikuj, do jakich celów wykorzystywane będą Twoje dane osobowe.
- Sprawdź, o jakie uprawnienia do danych jesteś proszony (np. lista kontaktów, lokalizacja) i ogranicz nadmiarowe uprawienia.
- Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna, tak aby inni uczestnicy konferencji ich nie zobaczyli.
- Korzystaj z opcji „poczekalnia" tak, abyś mógł kontrolować osoby dołączające się do telekonferencji, unikniesz przypadkowych lub nadmiarowych osób.
- Logując się do telekonferencji, wyłącz mikrofon i kamerę (włączysz je jak będzie to potrzebne).
- Po skorzystaniu z wideokonferencji wyłącz mikrofon i kamerę i upewnij się, że zakończyłeś spotkanie online i zamknąłeś aplikację. Program do telekonferencji może wciąż działać w tle.

Poczta elektroniczna

- Postępuj zgodnie z przyjętymi w organizacji zasadami dotyczącymi korzystania ze służbowej poczty elektronicznej.
- W celach służbowych używaj służbowych kont email. Jeśli pracując przetwarzasz dane osobowe i musisz używać prywatnego e-maila, upewnij się, że treść i załączniki są właściwie szyfrowane.
- Unikaj używania danych osobowych lub poufnych informacji w temacie wiadomości.
- Przed wysłaniem maila upewnij się, że wysyłasz go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe.
- Korzystaj z opcji UDW/BCC, adresaci dołączeni do pola UDW/BCC otrzymają kopię wiadomości, ale nie będą widoczni dla innych adresatów.
- Zawsze dokładnie sprawdź nadawcę maila. Nie otwieraj wiadomości od nieznanych adresatów, a zwłaszcza nie otwieraj załączników oraz nie klikaj w link zawarty w takiej wiadomości. To może być atak phishingowy.
- Nie przesyłaj mailem informacji zaszyfrowanej wraz z hasłem. Nawet w osobnej wiadomości. Ten kto ma dostęp do Twojej poczty bez problemu odszyfruje wiadomość.

Urządzenia

- Nie instaluj dodatkowych aplikacji i oprogramowania niezgodnych z przyjętymi w organizacji zasadami.
- Upewnij się, że wszystkie urządzenia, z których korzystasz, mają niezbędne aktualizacje systemu operacyjnego, oprogramowania oraz systemu antywirusowego.
- Zanim rozpoczniesz pracę, wydziel sobie odpowiednią przestrzeń, tak aby ewentualne osoby postronne nie miały dostępu do danych i dokumentów, nad którymi pracujesz. Odchodząc od stanowiska pracy każdorazowo blokuj urządzenia, na których pracujesz.
- Zabezpieczaj swój komputer poprzez używanie silnych haseł dostępu lub wieloskładnikowe uwierzytelnianie. Pozwoli to na ograniczenie dostępu do urządzenia, a jednocześnie na ograniczenie ryzyka utraty danych w przypadku kradzieży lub zgubienia urządzenia.
- Podejmij szczególne środki, aby urządzenia, z których korzystasz podczas pracy, szczególnie te wykorzystywane do przenoszenia jak dyski zewnętrzne, pamięci przenośne, nie zostały zgubione lub zniszczone.

Praca z dokumentami

- Dokumenty zawierające dane osobowe mogą być wynoszone poza teren organizacji tylko na wyraźne zlecenie pracodawcy.
- Należy zadbać o ewidencjonowanie wydanych pracownikom dokumentów zawierających dane osobowe.
- Udostępnione dokumenty muszą być przechowywane przez pracownika przez okres niezbędny do wykonania określonego zadania podczas pracy zdalnej – zasada ograniczenia przechowywania.
- Należy ograniczyć do niezbędnego minimum, w stosunku do celu przetwarzania danych osobowych przez pracownika w ramach pracy zdalnej, liczbę wynoszonych dokumentów.
- Należy zabezpieczyć dane osobowe podczas wynoszenia dokumentacji – przenoszenie dokumentów np. w taki sposób, aby były niewidocznie dla osób trzecich.
- Każdy pracownik powinien dbać o zabezpieczenie danych w miejscu wykonywania pracy zdalnej (np. przechowywanie dokumentów w zamykanych na klucz meblach, przestrzeganie zasady czystego biurka, zabezpieczenie dokumentów przed wglądem nieuprawnionych osób trzecich takich jak członkowie rodziny, współlokatorzy).
- Nie należy wyrzucać dokumentów zawierających dane osobowe do kosza. W przypadku, gdy pracownik nie posiada w domu niszczarki, dokumenty należy przechować w bezpieczny sposób, a po zakończeniu pracy zdalnej zniszczyć je w siedzibie organizacji.
- Należy zgłaszać pracodawcy każdy incydent bezpieczeństwa zgodnie z procedurą postępowania w sprawie naruszeń ochrony danych, tak aby administrator mógł się wywiązać z obowiązku nałożonego na mocy art. 33 ust. 1 RODO.

OTWARTY SYSTEM OCHRONY ZDROWIA

OSOZ

Wydawca: KAMSOFT S.A.
40–235 Katowice, ul 1 Maja 133
tel. +48 32 209-07-05
fax +48 32 209-07-15
e-mail: czasopismo@osoz.pl

Redaktor naczelny:
Artur Olesch

Jesteśmy partnerem
European Connected
Health Alliance

Zespół redakcyjny:
Karolina Szuścik.

Skład i łamanie: Piotr Chamera

BLOG OSOZ

Jeszcze więcej praktycznych informacji
znajdziesz na blogu OSOZ:

KAMSOFT

Rozwiązania dla Rynku Ochrony Zdrowia

SYSTEM SZPITALNY (HIS)

Jednym z najpopularniejszych systemów klasy HIS na rynku, jest **KS-MEDIS**, który zapewnia kompleksową obsługę szpitali, od procesów administracyjnych, poprzez zarządzanie magazynem i obrót lekami, aż po wsparcie procesów leczenia. KS-MEDIS, zapewnia również obsługę EDM oraz współpracuje z aplikacjami mobilnymi i systemami zewnętrznymi.

SYSTEMY WSPÓŁPRACUJĄCE Z KS-MEDIS

Aplikacje Mobilne dla Lekarzy i Pielęgniarek / **KS-ASW** (apteka szpitalna) / **KS-MediVeris**, **Systemy Finansowo-Księgowe** oraz **Kadrowo-Płacowe** z aplikacją mobilną dla pracowników **mZZL** / współpraca z **KS-SOLAB** (diagnostyka laboratoryjna).

SYSTEMY GABINETOWE

KAMSOFT oferuje szereg rozwiązań, które obsługują e-Recepty, EDM, eZLA, e-Skierowania, **obsługę szczepień przeciwko COVID-19 i grypie oraz są gotowe do rejestracji Zdarzeń Medycznych, indeksowania i wymiany EDM**. Dla dużych placówek i przychodni doskonale sprawdzi się system stacjonarny **KS-SOMED** lub chmurowy **SERUM**. Mniejsze podmioty, mogą także skorzystać z dobrze znanego programu **KS-PPS** (desktop) lub **Mediporta** (chmura).

ROZWIĄZANIA WSPÓŁPRACUJĄCE Z SYSTEMAMI GABINETOWYMI

Aplikacje mobilne dla lekarzy i pielęgniarek / **Rejestracja on-line** / **Telewizyty** / aplikacja mobilna dla pacjentów – **VisiMed** / powiadomienia SMS i w aplikacji VisiMed / **Wyniki Badań on-line** / współpraca z **KS-SOLAB** (diagnostyka laboratoryjna).

POZNAJ SYSTEMY KAMSOFT

E-ROZWIĄZANIA W OCHRONIE ZDROWIA

E-recepta, e-skierowanie, e-ZLA, eZWM, obsługa szczepień przeciwko Covid-19 i grypie to rozwiązania, które stały się nieodzownymi elementami pracy lekarzy i personelu medycznego. **Systemy KAMSOFT są również gotowe do rejestracji Zdarzeń Medycznych, indeksowania i wymiany EDM**. Więcej informacji dotyczących udostępniania i wymiany EDM na stronie edm.kamsoft.pl

RYNEK FARMACEUTYCZNY

Informatyzacja rynku farmaceutycznego w Polsce, rozpoczęła się od pierwszego wdrożenia systemu **KS-AOW**, w jednej z katowickich aptek na początku lat 90. Obecnie ponad 90% aptek korzysta z tego rozwiązania. KAMSOFT dostarcza również systemy do obsługi hurtowni farmaceutycznych **KS-HFW** oraz system umożliwiający weryfikację autentyczności produktów leczniczych **MediVeris** dla aptek, przychodni, hurtowni i szpitali.

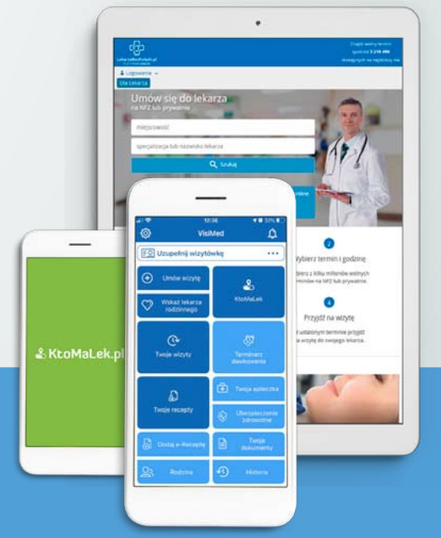
PACJENT

Rejestracja wizyt on-line, sprawdzenie dostępności leku w aptece, czy zdalne zamawianie recept to tylko niektóre z możliwości, jakie oferują pacjentom serwisy firmy KAMSOFT - **KtoMaLek.pl** oraz **LekarzeBezKolejki.pl**. Wspomniane funkcje łączy w sobie również aplikacja **VisiMed**, która ponadto umożliwia zrealizowanie bezdotykowej recepty w aptece, realizację telewizyty oraz prowadzenie harmonogramu dawkowania leków.

SERWISY WIDEO DLA SPECJALISTÓW

KAMSOFT jest również wydawcą serwisów **OSOZ-NEWS** i **OSOZ- TUTOR**. W ramach których eksperci KAMSOFT w przystępny sposób prezentują nowe funkcjonalności w systemach IT, aktualizacje związane ze zmianami w prawie oraz narzędzia wspomagające pracę lekarzy, pielęgniarek i farmaceutów. Materiały są publikowane codziennie na kanale youtube.pl oraz na dedykowanych stronach: **news.osoz.pl** / **tutor.osoz.pl**.

WŁĄCZ OSOZ-NEWS I BĄDŹ NA BIEŻĄCO



Rozwiązania KAMSOFT dla Rynku Zdrowia

Na co dzień pacjenci nie zdają sobie sprawy, jak to czego nie widać realnie wpływa na nasze zdrowie. Systemy informatyczne są tego doskonałym przykładem. Czy zastanawialiście się bowiem Państwo kiedykolwiek skąd w aptece wiadomo, co lekarz przepisał na recepcie, lub jak działa e-skierowanie? W KAMSOFT wiemy to doskonale bowiem od ponad 35 lat tworzymy te rozwiązania.

Codziennie z naszych systemów i aplikacji korzysta tysiące aptek i gabinetów lekarskich, setki szpitali oraz miliony pacjentów w całej Polsce. Wymiana informacji pomiędzy nimi jest możliwa również dzięki systemowi OSOZ (Otwarty System Ochrony Zdrowia), który integruje dane i łączy wszystkich uczestników rynku zdrowia.

KAMSOFT S.A. | ul. 1 Maja 133 | 40-235 Katowice | 32 209 07 05 | www.kamsoft.pl | biuro@kamsoft.pl