Ochrona danych na co dzień

Sprawdź nowe wytyczne i zadbaj o podstawy

W TYM WYDANIU:

Nowości w branży RODO - komentarz 1

Omówienie nowej opinii EROD 2

Nowy cykl

Czy Twój system ochrony danych ma solidne fundamenty? 5

Postawy prawne szyfrowania danych 7

Szyfrowanie - realizacja praktyczna 9

LexDigital

www.lexdigital.pl

Patrycja Żarska-Cynk

Komentarz do aktualnych wydarzeń w branży ochrony danych osobowych

Obowiązki podmiotów przetwarzających i podmiotów dalszego powierzenia - opinia EROD z 07.10.2024

Okazuje się, że mimochodem kontynuuję temat z poprzedniego newslettera dotyczący relacji pomiędzy administratorem danych osobowych a podmiotem przetwarzającym. A to w związku z kolejnymi ważnymi publikacjami dotyczącymi ochrony danych osobowych, które mają swój praktyczny wymiar.

EROD [Europejska Rada Ochrony Danych] przyjęła na początku października opinię w sprawie niektórych obowiązków Administratora danych osobowych wynikających z polegania na podmiotach przetwarzających i podprzetwarzających, czyli wskazówki dla podmiotów, które angażują podwykonawców/usługodawców w swoją działalność. Tym razem nie mówimy o **wytycznych** ale o **opinii** wydanej w następstwie wniosku złożonego do EROD przez duński organ ochrony danych na podstawie art. 64 ust. 2 RODO, na podstawie którego każdy organ ochrony danych może zwrócić się do Rady o wydanie opinii w sprawach mających ogólne zastosowanie lub wywołujących skutki w więcej niż jednym państwie członkowskim.

Dlaczego ma to znaczenie dla Twojej firmy?

Zatrudniając firmy zewnętrzne do obsługi zadań związanych z danymi osobowymi — takich jak lista płac, marketing lub usługi IT — pozostajesz odpowiedzialny za sposób przetwarzania tych danych. Nawet jeśli firmy te korzystają z podwykonawcy, to Twoja firma jest odpowiedzialna za zapewnienie zgodności z RODO.

Wspomniana opinia Europejskiej Rady Ochrony Danych (EDPB) wyjaśnia ważne obowiązki podczas pracy z podmiotami przetwarzającymi i podmiotami dalszego przetwarzania (firmami zatrudnionymi przez podmiot przetwarzający do pomocy w zadaniach związanych z danymi).

Opinia EROD

EROD w swojej opinii szczegółowo omawia, w jaki sposób administrator danych powinien zarządzać relacjami z podmiotami przetwarzającymi i podmiotami dalszego przetwarzania. Poniżej podsumowanie tez zawartych w dokumencie.

Wniosek 1

Administrator powinien znać tożsamość wszystkich podmiotów przetwarzających i podmiot dalszego przetwarzania w całym łańcuchu. Powinien mieć dostęp do informacji o nazwie, adresie i osobie kontaktowej każdego z nich, aby zapewnić zgodność z art. 28 RODO.

Wniosek 2

Administrator ma obowiązek zweryfikować, czy podmiot przetwarzający i podmioty dalszego przetwarzania zapewniają wystarczające gwarancje w zakresie ochrony danych. Ta weryfikacja powinna być odpowiednio udokumentowana i różnić się w zależności od ryzyka związanego z przetwarzaniem danych.

Wniosek 3

Administrator nie ma obowiązku systematycznie sprawdzać umów pomiędzy podmiotem przetwarzającym a podmiotem dalszego przetwarzania aby upewnić się, że obowiązki wynikające z RODO zostały przekazane w dół łańcucha przetwarzania, ale w zależności od okoliczności może być to konieczne, aby zapewnić zgodność z zasadą rozliczalności.

Wniosek 4

Administrator musi ocenić i mieć dostęp do odpowiedniej dokumentacji, która zapewnia, że poziom ochrony danych pozostaje zgodny z RODO, nawet podczas przekazywania danych do krajów trzecich

W pierwszej kolejności, gdy dane osobowe będą przekazywane do państw trzecich w związku z korzystaniem z usług (pod)podmiotów przetwarzających, administrator powinien ocenić i być w stanie przedstawić dokumentację dotyczącą mapowania przekazywania danych. Administrator powinien dopilnować, aby eksporter (który przetwarza dane osobowe w jego imieniu) przeprowadził mapowanie przekazywania, określając, które dane osobowe są przekazywane.

Wniosek 5

Zakres obowiązków Administratora w zakresie weryfikacji procesów może się różnić w zależności od tego jakie ryzyko dla praw i wolności osób niosą powierzone czynności przetwarzania. Im wyższe ryzyka tym weryfikacja bardziej szczegółowa, a środki bezpieczeństwa bardziej rygorystyczne.

Wniosek 6

Każda taka umowa powinna uwzględniać szczególne obowiązki administratorów i podmiotów przetwarzających. Chociaż art. 28 zawiera listę punktów, które muszą zostać uwzględnione w każdej umowie regulującej stosunki między administratorami i podmiotami przetwarzającymi, pozostawia on miejsce na negocjacje między stronami takich umów. Pole do negocjacji jest ograniczone wymogami określonymi w art. 28(3) RODO. Oznacza to, że klauzula przewidziana w art. 28 ust. 3 lit. a) RODO - "chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający" - jest zalecana, ale nie obowiązkowa. Jej brak nie oznacza automatycznego naruszenia RODO, ale umowa powinna jasno wskazywać, że procesor musi działać zgodnie z prawem UE lub krajowym.

Aby administrator danych osobowych zapewnił zgodność z opinią EROD dotyczącą relacji z procesorami i podprocesorami, w swojej polityce ochrony danych powinien wdrożyć następujące środki organizacyjne i techniczne:

Zastosowanie opinii EROD w praktyce w ramach systemu ochrony danych osobowych

Bądź RODOsmart. Proponuję Ci kilka elementów jakie warto uwzględnić na bazie wniosków z opinii EROD.

1 W procedurze wyboru dostawcy, w aktualnym projekcie karty oceny dostawcy:

a) Upewnij się, że uwzględniłeś informacje o dostawcy i wskazanych przez niego podwykonawcach w zakresie:

- nazwy firmy
- adresu siedziby
- osoby kontaktowej (imię, nazwisko, stanowisko, dane kontaktowe)
- kategorii dostawcy (opis jaki uwzględniasz w obowiązku informacyjnym)
- zakresu przetwarzania [przedmiot usługi lub części przedmiotu usługi realizowanego przez ten podmiot].

b) Upewnij się, że dokonałeś dywersyfikacji oczekiwanych środków organizacyjno-technicznych wobec dostawców w zależności od charakteru przetwarzanych danych oraz poziomu ryzyka.

c) Upewnij się, że w karcie dostawcy zawarłeś obowiązek zgłoszenia transferu danych poza UE. Dotyczy to zarówno dostawcy, jak i jego podwykonawców. Jeśli taki transfer ma miejsce, a w kraju odbiorcy nie ma decyzji Komisji Europejskiej o odpowiednim poziomie ochrony danych, musisz przeprowadzić ocenę wpływu transferu danych (Transfer Impact Assessment - TIA). Ocena ta powinna być wykonana przed podpisaniem umowy.

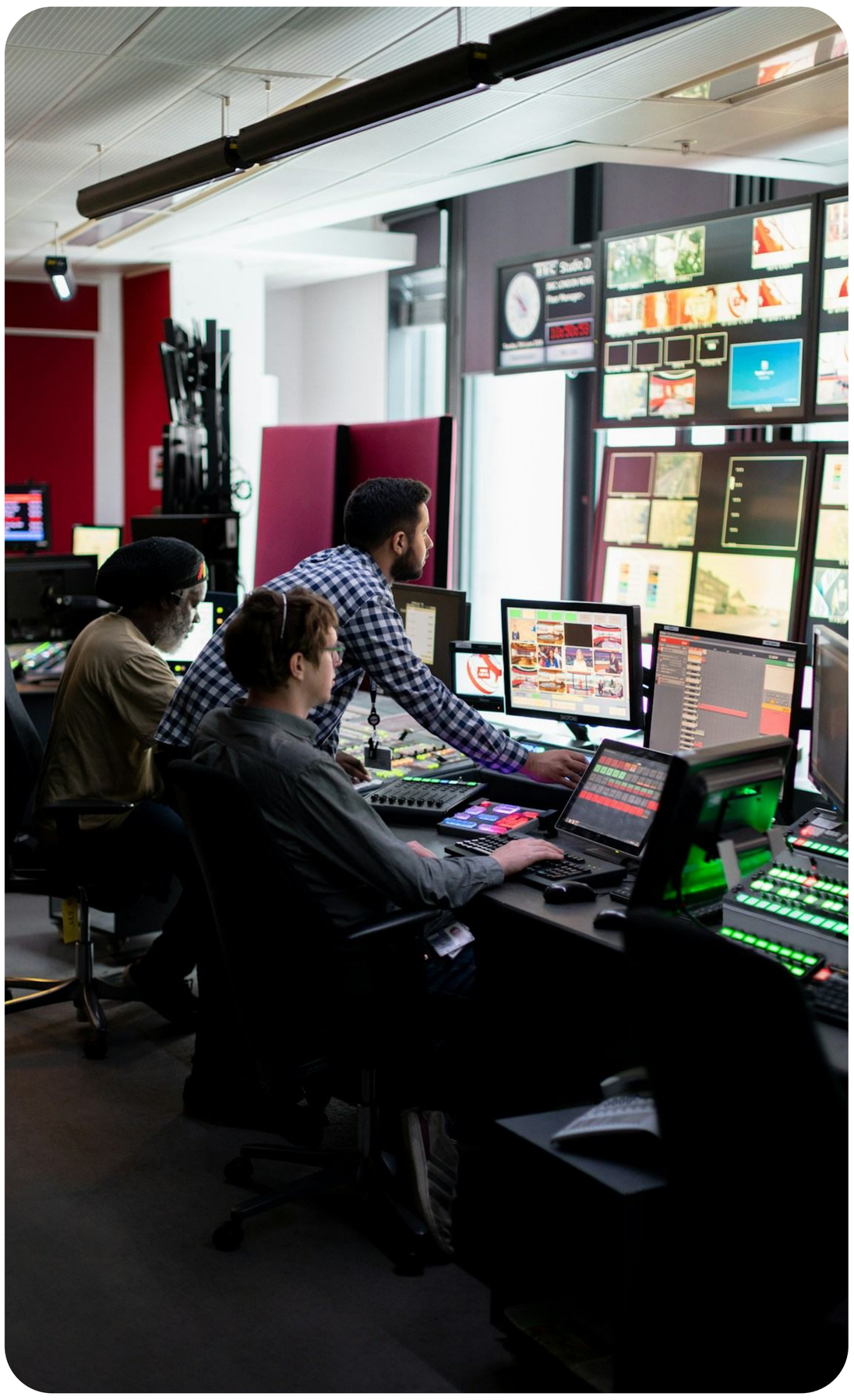
c) Upewnij się, że szablon umowy powierzenia przetwarzania danych jest zgodny z art. 28 RODO. Wprowadź do umowy wszystkie niezbędne zapisy, które muszą być uwzględnione. Zostaw przestrzeń na dodatkowe zapisy, które można negocjować z dostawcą. Nawet jeśli dostawca nie zaakceptuje Twojej wersji umowy, porównaj jego dokument z własnym projektem. Dzięki temu szybko zauważysz brakujące elementy lub te, które są dla Ciebie nie do przyjęcia.

2 W ramach procesów z obszaru utrzymania ciągłości działania i ciągłej analizy ryzyk dla przetwarzania danych:

a) Prowadź (w oparciu o karty dostawców, z którymi podpisano umowę) rejestr dostawców i poddostawców do nich przypisanych i regularnie aktualizuj te informacje.

b) Pamiętaj o udokumentowanej ocenie faktycznie stosowanych przez dostawców środków organizacyjno-technicznych i przestrzegania warunków umowy. Wyniki i daty oceny uwzględnij w rejestrze dostawców, co pomoże zaplanować ci kolejne działania:

- Przeprowadź i udokumentuj TIA, jeśli niezbędne, wracaj do tego dokumentu przy okazji audytu.
- Przeprowadź i udokumentuj audyt realizacji warunków umowy. Sprawdź, czy dostawca i podmioty dalszego przetwarzania stosują środki organizacyjno-techniczne, które zadeklarowali w umowie. Upewnij się, że działają wyłącznie na podstawie Twoich pisemnych instrukcji i czy przetwarzają dane tylko w zakresie określonym w umowie i w Twoim celu, a nie we własnych, które nie są przez Ciebie akceptowane.
- Regularnie sprawdzaj, czy podmioty przetwarzające informują Cię jako administratora danych o wszelkich zmianach w łańcuchu przetwarzania (np. dodanie nowego podmiotu dalszego przetwarzania).



Podsumowanie

Pamiętaj! Jeśli zatrudniasz dostawców, w tym takich, którzy opierają swoje usługi na łańcuchu podwykonawców, to odpowiedzialność za zgodność z RODO przetwarzania danych nie rozkłada się i nie regresuje a spoczywa na Tobie. Aby chronić swoją firmę i dbać o bezpieczeństwo danych osobowych przetwarzanych przez Twoją firmę, wypracuj sprawne mechanizmy działania przy wyborze dostawców. Wykorzystaj wnioski zawarte w opinii EROD, jak i innych wytycznych organów ochrony danych osobowych, co ułatwi ci organizację pracy. Przede wszystkim jednak, skoro korzystasz z profesjonalnego wsparcia w procesach biznesowych, to korzystaj też z profesjonalnego wsparcia organizacji i utrzymania zgodności z RODO Twojej firmy.

Źródło:

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_en

Maciej Kołodziej

Nowy cykl Czy Twój system ochrony danych na pewno ma solidne fundamenty?

Szyfrowanie informacji – wymóg w środowiskach nowych technologii

W dobie szybkiego rozwoju nowych technologii informatycznych, w związku z dynamicznie rozrastającymi się zasobami informacji przetwarzanej w rozproszonych systemach IT, łatwością zestawiania ze sobą danych pochodzących z różnych źródeł zlokalizowanych w cyberświecie oraz wyzwaniami związanymi z systemami wspomaganymi rozwiązaniami Sztucznej Inteligencji (AI), trudno jest zawsze zapewnić najwyższą, oczekiwaną jakość oferowanych rozwiązań. Złożoność wymagań biznesowych, zmiany formalno-prawne i ciągły pośpiech w wyścigu konkurencyjnym powodują, że projektanci systemów informatycznych oraz podmioty odpowiedzialne za nadzór nad przetwarzaniem danych nie zawsze uwzględniają w projektach fundamentalne wymogi stawiane systemom przetwarzania informacji. Zdarzają się sytuacje, gdy wymagane cechy związane np. z bezpieczeństwem są ograniczane a nawet pomijane, aby optymalizować koszty, skrócić czas powstania produktu, uprościć funkcjonalność usług lub parametry eksploatacji systemów. Takie decyzje (mimo sprzeciwu personelu odpowiedzialnego za kwestie bezpieczeństwa) często uzyskują akceptację biznesową, a weryfikacji adekwatności i skuteczności zastosowanych rozwiązań dokonuje użytkownik systemu produkcyjnego lub intruz, ingerujący w treść przetwarzanych danych.

Mając powyższe na uwadze pragniemy, równolegle do informowania o najnowszych trendach w dziedzinie cyberbezpieczeństwa i ochrony danych osobowych, przypominać również o fundamentalnych wymaganiach stawianych przed wdrażanymi w organizacjach systemami przetwarzania informacji.

Jednym z podstawowych zagadnień jest temat kryptografii, czyli szyfrowania i deszyfrowania danych. Polega na przetwarzaniu danych źródłowych do postaci szyfrogramu w taki sposób, żeby umożliwić zapoznanie się z ich treścią osobom i procesom do tego uprawnionym, ograniczając do minimum możliwość dostępu do informacji osobom trzecim. Aby szyfrowanie mogło być wykorzystywane, konieczne jest również opracowanie zasad deszyfrowania, czyli operacji odwrotnych, które pozwolą, na podstawie znajomości metody szyfrowania i wykorzystania odpowiednich atrybutów procesu (np. hasła, klucza deszyfrującego), na dostęp do treści źródłowych zawartych w szyfrogramie lub potwierdzenie faktów związanych

z przetworzoną i zawartą w szyfrogramie informacją. Istotnym jest także to, aby niezakłócony dostęp do danych, jeśli mają one znaczenie np. dla funkcjonowania procesów w organizacji, był możliwy również w przyszłości (zgodność użytej metody z kolejnymi stosowanych wersjami rozwiązań lub dbałość o dostępność wymaganych narzędzi) oraz w przypadku niedostępności osób uczestniczących w pierwotnym procesie utajniania (dysponowanie kluczami, aby zapewnić dostęp do danych organizacji nimi dysponującej lub większej ilości osób niż tylko twórca i adresat przekazu).

Szyfrowanie znajduje zastosowanie nie tylko podczas ochrony treści danych, ale również jako mechanizm wspomagający w procesach służących do ich przetwarzania, np. podczas:

- **przechowywania danych nieaktywnych** (tzw. dane w spoczynku, data in rest),
- **transmisji danych aktywnych** (tzw. dane w ruchu, data in motion/transit),
- **przetwarzania danych aktywnych** (tzw. dane w użyciu, data in use),
- **kontroli dostępu do systemów i danych,**
- **uwierzytelniania, zarządzania tożsamością i uprawnieniami,**
- **użytkowania mechanizmów ochrony** stanowisk roboczych, serwerów, magazynów danych i infrastruktury teleinformatycznej.
- **weryfikacji parametrów** istotnych operacyjnie lub biznesowo (np. potwierdzanie spójności lub autorstwa dokumentów).

Analizując zagadnienie szyfrowania w kontekście trzech podstawowych atrybutów informacji, czyli tzw. Triady CIA: poufność (ang. confidentiality), integralność (ang. integrity) i dostępność (ang. availability), będących fundamentem bezpieczeństwa w procesach przetwarzania danych, można wskazać, że stosowanie szyfrowania pozwala, między innymi, na zapewnienie:

- **Poufności danych**, jeżeli zastosowane zostaną odpowiednie mechanizmy, korzystające z nowoczesnych algorytmów szyfrowania przekształcających dane w taki sposób, że pozostaną one nieczytelne dla osób i procesów, które nie dysponują hasłem / kluczem przeznaczonym do rozszyfrowania informacji;
- **Integralności (spójności) danych**, zapewniając ochronę danych przed przypadkową lub intencjonalną modyfikacją ich zawartości (bez uprawnień lub bez wiedzy i zgody ich dysponenta), podczas ich przetwarzania, w tym przechowywania lub przesyłania;
- **Dostępności danych**, jeżeli stosowane procesy ochrony informacji będą uwzględniały również ochronę dostępu do treści danych i zabezpieczenie ich przed usunięciem lub trwałą, niezamierzoną modyfikacją.
- **Niezaprzeczalności danych**, która jest możliwa do wykazania, pod warunkiem stosowania odpowiednich rozwiązań kryptograficznych (np. technologii podpisów cyfrowych), podczas potwierdzania tożsamości autora lub źródła pochodzenia danych albo w czasie badania spójności dokumentu.
- **Ochrony danych przed niektórymi cyberatakami**, w których wektorem ataku jest treść informacji (np. czynności mające na celu zapoznanie się lub modyfikację przetwarzanych danych, takie jak „Man in The Middle" lub podsłuch pasywny podczas transmisji, albo dostęp lub modyfikacja treści przechowywanych w repozytoriach i bazach danych)

Podstawy prawne szyfrowania danych

Wśród istotnych regulacji dotyczących szyfrowania informacji wskazać należy te, które wprost powołują wymogi dotyczące kryptografii:

- Unijne **Rozporządzenie o ochronie danych** osobowych zaleca stosowanie szyfrowania, wymieniając je jako jeden z głównych środków minimalizujących ryzyko i zapewniających odpowiedni poziom bezpieczeństwa, w tym poufność, podczas przetwarzania danych osobowych oraz projektowania i utrzymania procesów (motyw 83, art. 25 i art. 32 ust. 1 a) RODO). Rozporządzenie nie opisuje dokładnie na czym szyfrowanie ma polegać i jak należy je stosować w procesach ochrony danych osobowych, pozostawiając decyzję w tym zakresie administratorom, jednak praktyka pokazuje, że szyfrowanie, oprócz funkcji bezpośredniej ochrony informacji, jest też składnikiem procedur pseudonimizacji, co wskazuje na duże znaczenie szyfrowania podczas spełniania wymogów stawianych przez RODO przed podmiotami przetwarzającymi dane osobowe.

- W polskim **Rozporządzeniu w sprawie Krajowych Ram Interoperacyjności** (tzw. KRI), będącym jednym z aktów wykonawczych do Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, zawarte zostały najważniejsze wymagania stawiane przed podmiotami świadczącymi elektroniczne usługi publiczne. W Rozdziale 4 Rozporządzenia KRI, wśród minimalnych wymagań dla systemów teleinformatycznych, wymienione zostały:
  - §16 ust.1 - konieczność wyposażenia używanych systemów teleinformatycznych w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach.
  - §18 ust.1 - udostępnianie zasobów informacyjnych w co najmniej jednym z formatów danych określonych w załączniku nr 2 do KRI, które wymieniono w liście w części B pkt. 3 „Do elektronicznego podpisywania, weryfikacji podpisu, opatrywania pieczęcią elektroniczną i szyfrowania dokumentów elektronicznych stosuje się: pkt. 3.1÷7”
  - §19 ust.1 - opracowanie, ustanowienie, wdrożenie i eksploatację, monitoring i przeglądy oraz utrzymanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji zapewniającego poufność, dostępność i integralność informacji (triada CIA) z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
  - §19 ust.2 pkt. 3) - przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
  - §19 ust.2 pkt. 12) d) - stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa.

Powyższe potwierdza znaczenie szyfrowania dla realizacji obowiązków nakładanych na podmioty zobowiązane do stosowania KRI.

- **W Ustawie o Krajowym Systemie Cyberbezpieczeństwa**, w rozdziale 3, wśród obowiązków operatorów usług kluczowych, zapisano konieczność wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanym do świadczenia usług kluczowych, zapewniającego stosowanie, m.in. odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, aby zapewnić ciągłe i niezakłócone świadczenie usług kluczowych, zapobiegać i ograniczać wpływ incydentów na bezpieczeństwo systemu informacyjnego oraz zapewnić poufność, integralność, dostępność i autentyczność informacji.

- **Normy ISO 27001 i 27002** przewidują konieczność przeprowadzenia kontroli organizacji w zakresie zarządzania zagrożeniami bezpieczeństwa informacji. W wykazie punktów kontroli bezpieczeństwa (nazywanym także listą zabezpieczeń), które mają być stosowane w celu poprawy bezpieczeństwa zasobów informacyjnych, znajduje się pozycja 8.24 odnosząca się do wykorzystywania kryptografii. Zabezpieczenie to wskazuje na potrzebę zdefiniowania i wdrożenia zasad skutecznego korzystania z kryptografii, w tym zarządzania kluczami kryptograficznymi, aby zapewnić właściwe i skuteczne wykorzystania kryptografii w celu ochrony poufności, autentyczności lub integralności informacji zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji oraz z uwzględnieniem wymogów prawnych, ustawowych, regulacyjnych i umownych związanych z kryptografią. Również zabezpieczenie 5.1, dotyczące wdrożenia zasad bezpieczeństwa informacji, zawiera wskazówki, aby Polityka Bezpieczeństwa Informacji była uzupełniona o polityki tematyczne, które powinny obejmować określone obszary bezpieczeństwa. Jako jeden z przykładów wskazana została polityka dotycząca kryptografia i zarządzania kluczami.

- Unijna **Dyrektywa NIS2** (Network and Information Security Directive 2) to druga odsłona regulacji unijnej dotyczącej bezpieczeństwa sieci i informacji. W motywie 51 preambuły znalazł się zapis o korzystaniu z innowacyjnych technologii, w tym sztucznej inteligencji, których stosowanie mogłoby poprawić wykrywanie i zapobieganie cyberatakom. Wskazano, że istotnym zagadnieniem jest zapewnienie bezpieczeństwa danych, które wspomagają nowoczesne metody szyfrowania, a ich stosowanie wynika z obowiązującego prawa. Zaleca się promowanie stosowania szyfrowania podczas transmisji danych (motyw 98) oraz do ochrony urządzeń końcowych (motyw 104). Cyberbezpieczeństwo w kontekście ochrony danych osobowych, w związku z RODO i przepisami powiązanymi, zostało opisane w motywie 121, a w artykule 21 wśród środków zarządzania ryzykiem w cyberbezpieczeństwie wymieniono polityki i procedury dotyczące stosowania kryptografii.

- Rozporządzenie europejskie w sprawie operacyjnej odporności cyfrowej **(Rozporządzenie DORA**) określa ramy kompleksowego zarządzania ryzykiem cyfrowym na rynkach finansowych. Kwestie szyfrowania informacji, w kontekście zarządzania ryzykiem związanych z ICT (ang. Information and Communication Technologies, Technologie teleinformatyczne dotyczące przesyłania, gromadzenia, przetwarzania i prezentacji informacji w systemach elektronicznych) dotyczą m.in. polityk dotyczących mechanizmów uwierzytelniania oraz środków ochrony kluczy kryptograficznych, dzięki którym dane szyfruje się na podstawie wyników zatwierdzonych procesów klasyfikacji danych i oceny ryzyka. Procesy te powinny być nadzorowane i rozwijane, zgodnie z zaleceniami wydawanymi w porozumieniu z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), przez Europejski Urząd Nadzoru finansowego (EUN) i organy nadzorcze.

Realizacja praktyczna

Mając świadomość celu i znaczenia szyfrowania dla funkcjonowania systemów ochrony informacji należy odpowiednio zidentyfikować obszary, w których w organizacji zachodzi potrzeba wdrożenia kryptografii oraz określić ich istotność dla poszczególnych składowych procesu.

Identyfikację można przeprowadzić według kryteriów:

- **Sposobu przetwarzania danych:**
  - Przechowywanie danych nieaktywnych (dane w spoczynku, data in rest): składowanie zaszyfrowanych danych zapisanych na nośnikach pamięci w urządzeniach lub magazynach danych, na nośnikach przenośnych lub w chmurach (cloud encryption), oraz w kopiach zapasowych i archiwach,
  - Transmisja danych aktywnych (dane w ruchu, data in motion/transit): bezpieczne przesyłanie danych za pośrednictwem sieci komputerowych, ochrona dostępu do danych przetwarzanych w pamięci RAM urządzeń, przysyłanie zaszyfrowanych informacji jako składniki różnych form komunikacji,
  - Przetwarzanie danych aktywnych (dane w użyciu, data in use): ochrona operacji na danych ulegających zmianom, bezpiecznie tworzonych, kasowanych, przeglądanych przez użytkowników i procesy; szyfrowanie danych zapisywanych na nośnikach, w bazach danych lub w zasobach dostępnych dla poszczególnych procesów,

- **Miejsca przetwarzania danych:**
  - Nośniki: pendrive'y, płyty CD/DVD, dyski – manualna lub automatyczna ochrona zapisywanych treści
  - Stacjonarne urządzenia końcowe: komputery – ochrona dostępu do kont i urządzenia, szyfrowanie nośników, katalogów lub pojedynczych plików, separacja zasobów użytkowników, konfiguracja szyfrowania danych przetwarzanych w aplikacjach, konfiguracja bezpiecznych protokołów i metod komunikacji pomiędzy aplikacjami po stronie klienta i obsługującymi go serwerami;
  - Mobilne urządzenia końcowe: laptopy, tablety, telefony komórkowe – ochrona dostępu do kont i urządzenia, zabezpieczenie nośników danych (wewnętrznych i dodatkowych, np. kart pamięci), konfiguracja i niezbędna separacja, domyślna odmowa, dostępu aplikacji do zasobów,
  - Serwery – ochrona dostępu do kont i urządzenia, szyfrowanie nośników, separacja procesów,
  - Macierze i magazyny danych – segmentacja i separacja struktur przechowywania danych,
  - Bazy danych – ochrona dostępu do danych i aplikacji, szyfrowanie struktur i nośników służących do przechowywania danych,
  - Systemy chmurowe (cloud computing) – ochrona dostępu, gdy to możliwe przetwarzanie danych zaszyfrowanych po stronie klienta usług,
  - Archiwa – szyfrowanie zawartości depozytów archiwalnych jako zabezpieczenie przed dostępem osób nieuprawnionych;

- **Użytych narzędzi i rozwiązań kryptograficznych:**
  - Wybór i zatwierdzenie narzędzi i rozwiązań stosowanych w procesach szyfrowania i ochrony informacji – programy szyfrujące dane, archiwizery, technologie ochrony kanałów komunikacyjnych i dostępu do sieci, wersje bibliotek wykorzystywanych do szyfrowania, dobór wymaganej w organizacji siły rozwiązań kryptograficznych,
  - Szyfrowanie zasobów informacyjnych (z użyciem oprogramowania lub wsparcia sprzętowego) będących w spoczynku, w użyciu oraz podczas transmisji;
  - Stosowane mechanizmy uwierzytelniające:
    - hasła, PIN-y, dane poufne i zarządzanie nimi (np. sejfy lub depozyty),
    - klucze fizyczne, tokeny, karty identyfikacyjne,
    - biometria,
    - uwierzytelnienie wieloskładnikowe;
  - Konfiguracje bezpieczeństwa – ochrona informacji dotyczących stosowanych metod oraz konfiguracji narzędzi służących do szyfrowania, repozytoria haseł/kluczy krypotograficznych, polityki dotyczące zarządzania procesami kryptograficznymi oraz zarządzania ich atrybutami bezpieczeństwa;

PAMIĘTAJ!

Jeśli korzystasz z symetrycznego szyfrowania danych i używasz hasła służącego również do ich odszyfrowania, a przesyłasz szyfrogram (zaszyfrowaną treść danych) do innej osoby, to hasło pozwalające na poznanie zawartości przesyłki przekaż adresatowi w innym kanale komunikacji (np. SMS-em, telefonicznie) lub ustal wcześniej zasady jego tworzenia.

Dla podniesienia jakości stosowanych zabezpieczeń zaplanuj, jeśli istnieje taka możliwość, okresowe zmiany kluczy/haseł wykorzystywanych w procesach szyfrowania informacji.
Staraj się nie używać tych samych kluczy/haseł w różnych procesach i podczas dostępu do różnych zasobów teleinformatycznych. Korzystaj z rozwiązań wspierających zarządzaniem kluczami szyfrującymi, np. repozytoria lub sejfy haseł.

Podczas analizy ryzyka, w fazie projektowania oraz użytkowania rozwiązań kryptograficznych, staraj się dobrać dla każdego procesu przetwarzania danych rozwiązania optymalne i uznawane za skuteczne pod względem bezpieczeństwa. Niezwłocznie udoskonalaj stosowane mechanizmy, gdy dowiesz się o ich słabych stronach (np. o podatnościach dotyczących możliwości kompromitacji ochrony informacji).

Szyfrowanie to mechanizm wykorzystywany w wielu procesach (od składowania i przesyłania, po przetwarzanie danych). Nieskuteczna ochrona informacji lub jej brak na jednym z etapów może wywołać w Twojej organizacji negatywne skutki operacyjne, wizerunkowe, biznesowe lub prawne.

Podsumowując

Szyfrowanie danych, ich treści oraz w trakcie ich przetwarzanych w procesach informatycznych, stanowi ważny element składowy systemów bezpieczeństwa informacji, którego stosowanie powinno być traktowane jako obowiązek każdego podmiotu przetwarzającego informacje, także w sytuacji gdy nie ciąży na nim obowiązek wynikający z przepisów prawa.

Ponieważ szyfrowanie danych, przy braku właściwej ochrony zastosowanych kluczy szyfrujących, jest jedynie zabezpieczeniem pozornym, konieczne jest właściwe zaprojektowanie każdego procesu szyfrowania, ze szczególną dbałością o ochronę atrybutów bezpieczeństwa (metody szyfrowania oraz stosowanych kluczy/haseł), aby z szyfrowaniem można było powiązać gwarancję zapewnienia poufności przetwarzanej informacji.

Stosuj obowiązujące przepisy oraz korzystaj z dobrych praktyk i wskazówek dotyczących zasad ochrony informacji w kontekście ich bezpiecznego przetwarzania i szyfrowania w systemach teleinformatycznych.

W przypadku wątpliwości co do potrzeby stosowaniu lub doboru rodzaju ochrony kryptograficznej przeprowadź analizę ryzyka i podejmij decyzję w kontekście każdego procesu lub zestawu przetwarzanych danych.

Newsletter RODO

Październik 2024 nr 11/2024

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI

LexDigital

www.lexdigital.pl LinkedIn