Wymiana doświadczeń

Jarosław Pudzianowski - Pełnomocnik do Spraw Zarządzania Bezpieczeństwem

Warszawa, 2017-04-21

Centrum Systemów Informacyjnych
Ochrony Zdrowia

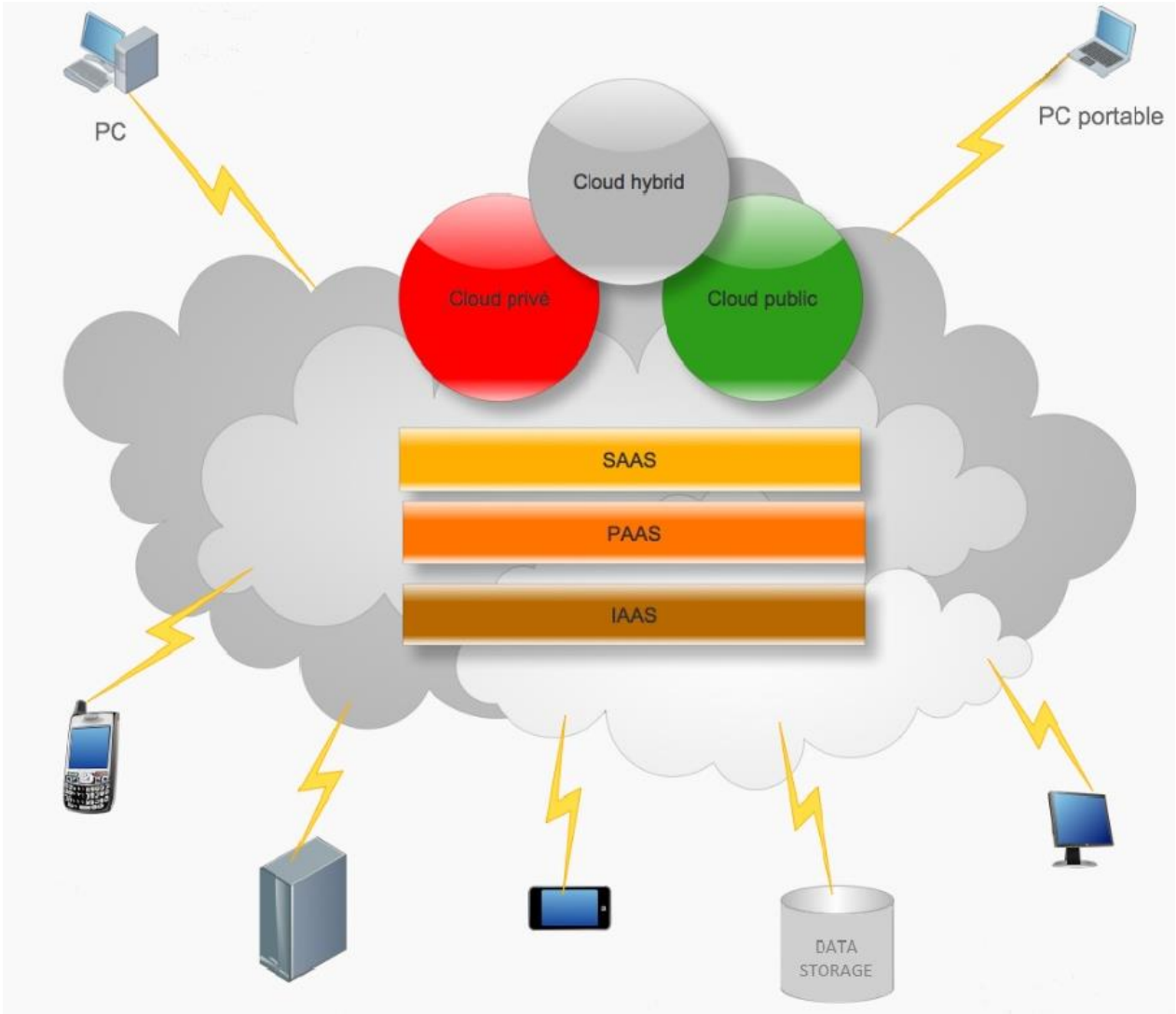
1. BEZPIECZEŃSTWO PRZETWARZANIA INFORMACJI W SYSTEMACH INFORMATYCZNYCH

Bezpieczeństwo informacji

Każdy z interesariuszy systemów jest zainteresowany uzyskaniem jak najwyższej jakości informacji (integralność i dostępność) oraz ochronie tej informacji przed nieupoważnionym dostępem (poufność).

Dotyczy to w szczególności danych o zdarzeniach medycznych, które są prawnie chronione jako dane osobowe wrażliwe.

Przetwarzanie informacji w chmurze



Przetwarzanie informacji w chmurze

Rozróżniamy trzy podstawowe rodzaje chmur:

- prywatne (ang. private cloud) – rodzaj chmur stanowiących część organizacji, uruchamiane i zarządzane w środowisku organizacji,

- publiczne (ang. public cloud) – rodzaj chmur, które są dostarczane przez zewnętrznego dostawce,

- hybrydowe (ang. hybrid) – połączenie chmury prywatnej i publicznej, gdzie część pracuje w środowisku organizacji a część w środowisku publicznym.

Przetwarzanie informacji w chmurze

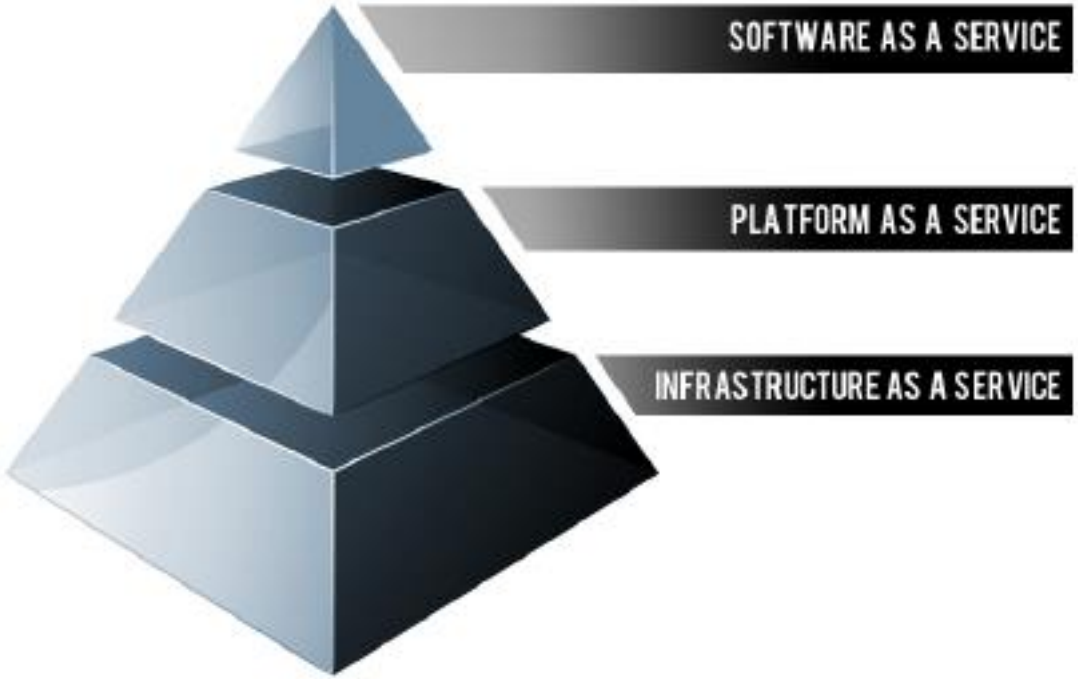
Modele chmury obliczeniowej

Najczęściej spotykanymi modeli chmury obliczeniowej są:

- Software as a Service (SaaS) – organizacja korzysta z aplikacji umieszczonych w chmurze. Kontrola podstawowej infrastruktury, w tym również zasobów sieciowych, serwerów, systemów i składowania danych znajduje się w kompetencjach i odpowiedzialności dostawcy.
- Platform as a Service (PaaS) – cechą charakterystyczną jest umożliwienie instalacji własnych aplikacji i systemów w infrastrukturze dostawcy.
- Infrastructure as a Service (IaaS) – cechą charakterystyczną jest dostarczanie podstawowych zasobów obliczeniowych, sieciowych, przechowywania danych i innych. W tym modelu istnieje możliwość instalowania i uruchamiania dowolnego oprogramowania.

Przetwarzanie informacji w chmurze

Odpowiedzialność



Przetwarzanie informacji w chmurze

Odpowiedzialność

Tak ułożone modele tworzą stos nazywany w skrócie SPI (S>P>I), w którym im niżej stosu dostawca dostarcza usługę tym organizacja jest w większym stopniu odpowiedzialna za zarzadzanie ryzykiem i zabezpieczeniem środowiska.

Można również umownie przyjąć, że odpowiedzialność dostawcy i organizacji w modelu IaaS kształtuje się w stosunku 50/50, w modelu PaaS odpowiedzialność dostawcy wzrasta aby w modelu SaaS osiągnąć najwyższy poziom, pozostawiając po stronie organizacji odpowiedzialność tylko za interfejs użytkownika.

Przetwarzanie informacji w chmurze

Odpowiedzialność

	Infrastruktura zarządzana przez:	Infrastruktura w posiadaniu:	Infrastruktura umieszczona :	Dostępna i wykorzystywana przez :
Publiczna	Dostawca	Dostawca	Na zewnątrz	Niezaufana strona
Prywatna/ Współdzielona	Organizacja Lub Dostawca	Organizacja Dostawca	Wewnątrz Na zewnątrz	Zaufana strona
Hybrydowa	Zarówno Organizacja jak i Dostawca	Zarówno Organizacja jak i Dostawca	Zarówno Wewnątrz jak i Na zewnątrz	Zarówno Zaufana i Niezaufana strona

Analiza ryzyka

Analiza ryzyka jest jednym z elementów procesu zarządzania ryzykiem. Wykonuje się ją podczas projektowania sytemu/sieci TI, cyklicznie w trakcie eksploatacji oraz w przypadku zaistnienia incydentu naruszenia bezpieczeństwa TI. W oparciu o wyniki analizy ryzyka dobiera się zabezpieczenia. Zastosowane zabezpieczenia powinny być efektywne kosztowo i uwzględniać wymagania wynikające z przepisów prawa, wymagania biznesowe i wymagania z analizy ryzyka zasobów posiadających wartość dla działania instytucji. Ryzyko jakie powstaje po wprowadzeniu zabezpieczeń nazywamy ryzykiem szczątkowym.

Aby poprawnie przeprowadzić analizę ryzyka potrzebujemy określonej wiedzy. Musi być nam znana polityka bezpieczeństwa wdrożona w danej jednostce organizacyjnej (np. kontrola dostępu do pomieszczeń lub monitoring), musimy wiedzieć co chronimy i przed kim/czym, a także konieczna jest wiedza na temat środków jakimi dysponujemy (ludzie, pieniądze, czas).

Analiza ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak aby to ryzyko zminimalizować lub całkowicie go zlikwidować.

Analiza ryzyka

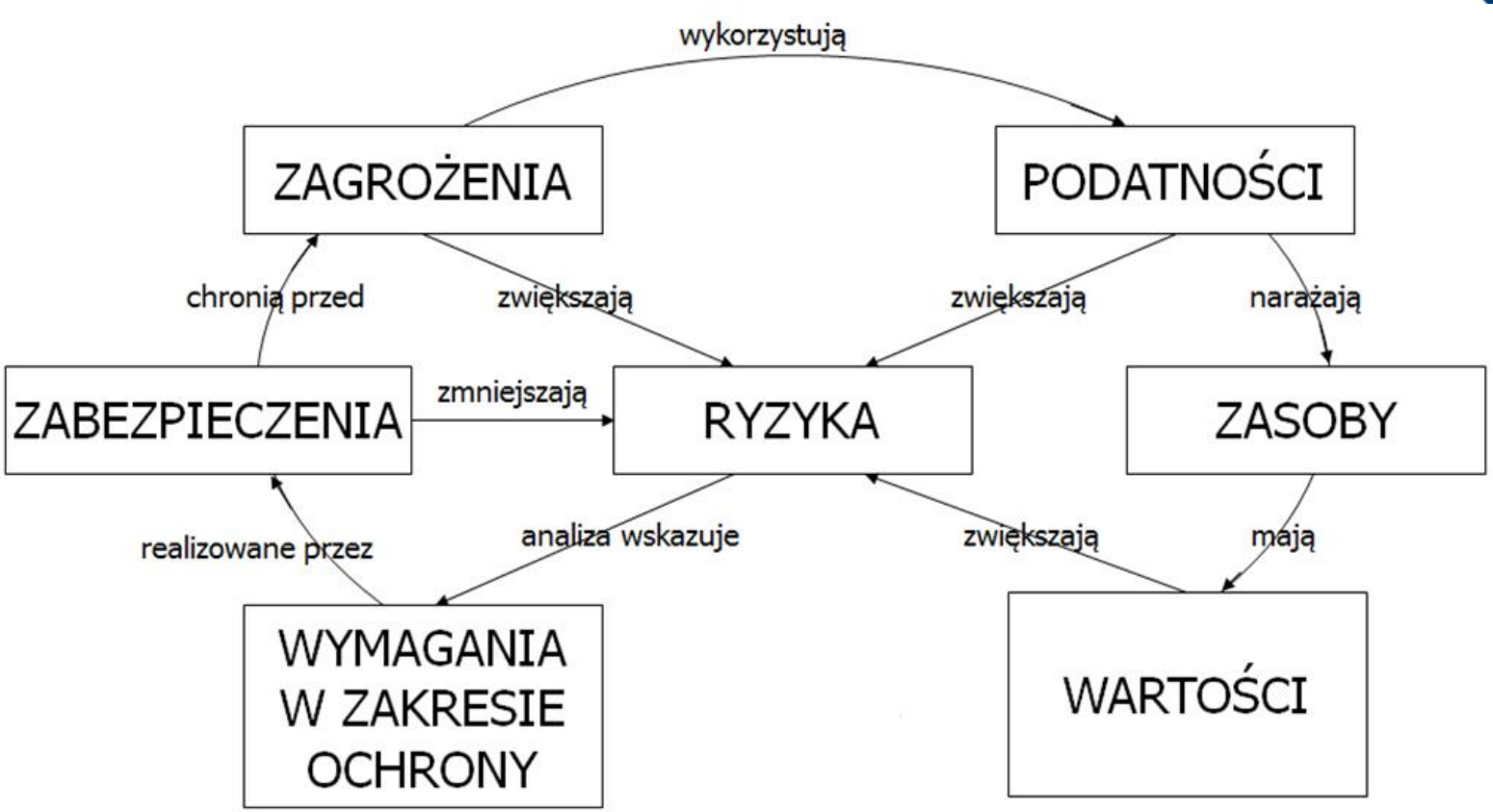
Aby przeprowadzić poprawnie analizę ryzyka na początku należy określić:

- zasoby, które będziemy chronić;
- zagrożenia – czynnik, który może powodować wystąpienie incydentu;
- podatność – słabość zasobów, która może być wykorzystana przez zagrożenie;
- skutki – jaki wpływ będzie miał zaistniały incydent na system/sieci TI.

Uzbrojeni w taką wiedzę możemy zacząć szacować ryzyko, które w dalszej fazie pozwoli wysunąć nam wnioski do dokumentacji bezpieczeństwa systemu.

Zasobami systemu są wszystkie elementy służące do przetwarzania, przechowywania, lub przekazywania informacji oraz do zapewnienia im właściwego poziomu bezpieczeństwa.

Analiza ryzyka
Postępowanie z ryzykiem



Przetwarzanie Informacji

Bezpieczeństwo

Poufność odnosi się do stosowania rozwiązań kryptograficznych.

Warto pamiętać że w modelu IaaS, klient usługi w chmurze nie może polegać na rozwiązaniu szyfrowania oferowanym przez dostawcę usługi w chmurze, ale może zdecydować się na szyfrowanie danych osobowych przed wysłaniem ich do chmury.

Również w zakresie komunikacji pomiędzy dostawca usługi a klientem wymagane jest stosowanie autoryzacji i uwierzytelniania, natomiast pomiędzy ośrodkami wymiany danych komunikacja powinna być zaszyfrowana.

Przetwarzanie informacji

Bezpieczeństwo

Integralność jest właściwością polegającą na zapewnieniu dokładności i kompletności aktywów co odnosząc wprost do danych oznacza, że są one prawdziwe i nie zostały złośliwie lub przypadkowo zmienione podczas przetwarzania, przechowywania lub przekazywania.

Naruszenia integralności danych przetwarzanych w chmurze można wykryć lub im zapobiec przy pomocy systemów służących wykrywaniu/zapobieganiu włamaniom (IPS/IDS) jako funkcji często występujących w urządzeniach klasy UTM.

Przetwarzanie informacji

Bezpieczeństwo

Dostępność tzn. właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

Zagrożeniem dla dostępności usług uruchomionych w środowisku chmurowym jest chociażby atak z wykorzystaniem DoS (odmowa usługi), dlatego administratorzy danych w celu zapewnienia ciągłości działania powinni zapewnić sobie prawo do kontroli w zakresie zastosowanych środków bezpieczeństwa w tym m.in.: łączy zapasowych, nadmiarowych zasobów oraz skutecznych mechanizmów wykonywania kopii zapasowych.

Przetwarzanie informacji

Bezpieczeństwo

Najważniejszym w kontekście zapewnienia bezpieczeństwa przetwarzanym informacjom jest wskazanie procesów, w których dane są przetwarzane, funkcje jakie pełnią w organizacji, danych oraz aplikacji służących do ich przetwarzania.

Przetwarzanie informacji

Model bezpieczeństwa

- Identyfikacja wymagań zewnętrznych i wewnętrznych,
- Określenie zakresu funkcjonowania,
- Opracowanie strategii,
- Wdrożenie Polityki Bezpieczeństwa,
- Monitorowanie i doskonalenie.

Przetwarzanie informacji

Etapy budowania bezpieczeństwa

- Wskazanie ról i odpowiedzialności za zarządzanie bezpieczeństwem,
- Określenie wymagań i kompetencji,
- Identyfikacja aktywów,
- Ustanowienie procesu oceny pod kątem integralności, dostępności i integralności przetwarzanych danych – analiza ryzyka,
- Analiza i ocena ryzyka,
- Postępowanie z ryzykiem

Przetwarzanie informacji

Etapy budowania bezpieczeństwa

- Ustanowienie Polityki Bezpieczeństwa Informacji
- Zapewnienie ochrony przetwarzanej informacji
- Monitorowanie i doskonalenie
- Podejmowanie działań korygujących.

Przetwarzanie informacji

Wytyczne, zasady i rekomendacje budowania bezpieczeństwa

- **Bezpieczeństwo fizyczne i środowiskowe**
  - Obszary bezpieczne
  - Bezpieczeństwo sprzętu
  - Lokalizacja sprzętu
  - Systemy wspomagające
  - Bezpieczeństwo okablowania
  - Konserwacja sprzętu
  - Obsługa nośników
  - Bezpieczeństwo sprzętu poza siedzibą
  - Bezpieczna likwidacja sprzętu
  - Wynoszenie sprzętu poza siedzibę organizacji
- **Bezpieczeństwo sieciowe**

Przetwarzanie informacji

Wytyczne, zasady i rekomendacje budowania bezpieczeństwa

- **Bezpieczeństwo systemów**
  - Ochrona antywirusowa
  - Usługi dostarczane przez strony trzecie
  - Planowanie i odbiór systemów
  - Zarzadzanie zmianą
  - Szyfrowanie danych medycznych

- **Kontrola dostępu**
  - Zarzadzanie tożsamością (uwierzytelnianie)
  - Zarządzanie dostępem użytkowników
  - Odpowiedzialność użytkowników
  - Kontrola dostępu do aplikacji
  - Kontrola dostępu do sieci
  - Praca na odległość, wykorzystywanie urządzeń przenośnych

Przetwarzanie informacji

Wytyczne, zasady i rekomendacje budowania bezpieczeństwa

- **Stosowanie podpisu elektronicznego**
- **Audytowalność i niezaprzeczalność danych i zdarzeń w systemie**
- **Archiwizacja danych medycznych**
- **Zarządzanie incydentami związanymi z bezpieczeństwem informacji**
- **Zarządzanie ciągłością działania**
  - Tworzenie i odtwarzanie kopii zapasowych
  - Dostępność i niezawodność (SLA)
  - Postępowanie na wypadek awarii/katastrofy i utraty danych
  - Plany BCP i DRP

INCYDENTY W BEZPIECZEŃSTWIE INFORMACJI

Postępowanie z incydentami bezpieczeństwa informacji stanowi bardzo ważny element programu zarządzania bezpieczeństwem informacji.

Wraz z procesami zarządzania ryzykiem (ang. *risk management*), zarządzania zdarzeniami bezpieczeństwa (ang. *security event management*), zarządzania podatnościami (ang. *vulnerability management*) i testami bezpieczeństwa, ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa aktywów informacyjnych na działalność przedsiębiorstwa, w tym na ciągłość operacyjną jego procesów biznesowych, systemów i infrastruktury teleinformatycznej.

INCYDENTY W BEZPIECZEŃSTWIE INFORMACJI

Incydentem bezpieczeństwa informacji jest zdarzenie, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych.

W szczególności incydentami bezpieczeństwa informacji są:

- przypadki naruszenia poufności (ujawnienie niepowołanym osobom), integralności (uszkodzenie, przekłamanie, zniszczenie) i dostępności (dane nie są dostępne w użytecznej postaci na żądanie uprawnionych użytkowników) danych, niezależnie od ich nośnika, w tym także przechowywanych i przetwarzanych w systemach informatycznych oraz transmitowanych przez łącza sieci;

INCYDENTY W BEZPIECZEŃSTWIE INFORMACJI

- niedostępność oraz działania niezgodne ze specyfikacją (błędne) systemów informatycznych, zwłaszcza systemów i aplikacji krytycznych (z wyłączeniem kontrolowanych i zaplanowanych prac oraz dysfunkcji niemających wpływu na bezpieczeństwo informacji;
- infekcje, propagacja i działanie szkodliwego oprogramowania (malware – kody i skrypty mające szkodliwe, przestępcze lub złośliwe działanie, do których zaliczają się miedzy innymi wirus, robak internetowy, koń trojański, spyware, keylogger, rootkit, dialer, exploit etc.);
- rozpoznanie, penetracja i próby omijania systemów zabezpieczeń;
- niewłaściwe wykorzystywanie lub nadużywanie zasobów informacyjnych;

INCYDENTY W BEZPIECZEŃSTWIE INFORMACJI

- ataki nieautoryzowanego dostępu do aplikacji, systemów oraz ataki eskalacji poziomu uprawnień w systemach;
- kradzież lub zniszczenie urządzeń przetwarzających lub/i przechowujących informacje oraz nośników danych;
- wyłudzenia (lub próby wyłudzeń) informacji wrażliwych, takich jak np. hasła dostępowe czy tajemnice przedsiębiorstwa;
- ataki socjotechniczne, ataki z wykorzystaniem phishing'u, skimming'u oraz innych technik zagrażających naruszeniu poufności, dostępności i integralności informacji;
- incydenty wielokomponentowe (złożone incydenty dotyczące wielu systemów, wykorzystujące wiele wektorów ataków itp.);

Przetwarzanie informacji

Cyberbezpieczeństwo, Infrastruktura krytyczna i ciągłość działania

Dyrektywa NIS (Dyrektywa Parlamentu i Rady UE 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii przyjęta została 6 lipca 2016 roku.) zakłada poszerzenie współpracy państw członkowskich w kwestii cyberbezpieczeństwa.

Jednym z sektorów objętych dyrektywą jest sektor e-zdrowia zawierający zagadnienia dotyczące przetwarzania dokumentacji medycznej w postaci elektronicznej . Dyrektywy PE i Rady (UE) 2016 /1148 z dn. 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów teleinformatycznych

Przetwarzanie informacji

Cyberbezpieczeństwo, Infrastruktura krytyczna i ciągłość działania

Zgodnie z Dyrektywą NIS konieczne jest zapewnienie przez poszczególne podmioty mające udział w przetwarzaniu informacji minimalnego poziomu ochrony dla infrastruktury w tym sieci i systemów przetwarzających dokumentacje medyczną. Poprzez realizację tego wymogu rozumieć należy wdrożenie odpowiednich środków bezpieczeństwa w warstwie organizacyjnej, technicznej i systemowej oraz w przypadku wystąpienia poważnych incydentów bezpieczeństwa informacji podjęcie odpowiednich działań ograniczających ich skutki, a co najważniejsze powiadomienie krajowego organu cyberbezpieczeństwa jakim jest CERT Polska. Krajowy organ będzie mógł nakładać sankcje na podmioty, które nie dostosują się do Dyrektywy NIS i nie wdrożą zabezpieczeń zapewniających spełnienie minimalnego poziomu bezpieczeństwa sieci i systemów.

Przetwarzanie informacji

Cyberbezpieczeństwo, Infrastruktura krytyczna i ciągłość działania

Dyrektywa NIS nakłada na kraje członkowskie obowiązek zachowania ciągłości funkcjonowania infrastruktury krytycznej, a co za tym idzie nakłada na podmioty odpowiedzialność za ciągłość działania i świadczenie tzw. usług krytycznych.

W sektorze e-zdrowia są to usługi związane z zapewnieniem:

- ciągłości działania systemów informacji zdrowotnej przetwarzającej elektroniczną dokumentację medyczną,
- dostępnością repozytoria danych czyli bazy danych w jednostkach, w którym informacja jest przechowywana lokalnie,
- dostępnością dla użytkowników systemów informatycznych realizowaną między innymi poprzez ciągłość pracy serwerów odpowiedzialnych uwierzytelnianie tj. przeprowadzenie kontroli dostępu i uwierzytelniania użytkowników,
- ciągłości działania informatycznych systemów laboratoryjnych - Laboratory Information System (LIS)
- ciągłości działania informatycznych systemów radiologicznych - Radiology Information Systems (RIS)
- dostępności elektronicznej dokumentacji medycznej zawartych w elektronicznych kartach zdrowia,
- kluczowych usług niezbędnych do świadczenia opieki zdrowotnej.

Dziękuję za uwagę.

e-mail: wspolpraca-regiony@csioz.gov.pl

Centrum Systemów Informacyjnych
Ochrony Zdrowia