STANDARD CYBERBEZPIECZEŃSTWA PPBW

DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW ORAZ INSTYTUCJI PUBLICZNYCH

POLSKA PLATFORMA BEZPIECZEŃSTWA WEWNĘTRZNEGO

STANDARD CYBERBEZPIECZEŃSTWA PPBW DLA MŚP I INSTYTUCJI PUBLICZNYCH

SPIS TREŚCI

03

WSTĘP

Standard cyberbezpieczeństwa został opracowany w celu wskazania modelowych rozwiązań w zakresie ustanawiania, wdrażania, monitorowania i doskonalenia poziomu cyberbezpieczeństwa w małych i średnich przedsiębiorstwach oraz w instytucjach publicznych. Standard czerpie silnie z istniejących i uznanych norm, dostosowując je do specyfiki i uwarunkowań funkcjonowania wyżej wymienionych podmiotów.

Standard składa się z czterech etapów:

1. Zarządzanie aktywami informacyjnymi (więcej zał. 1 na przykłady aktywów informacyjnych).
2. Zarządzanie ryzykiem.
3. Wybór zabezpieczeń i ich implementacja.
4. Testowanie bezpieczeństwa, monitoring, audyt, ciągłe doskonalenie.

Etapy podzielone zostały na składające się na nie zadania. Dodatkowo etap II podzielony został na cztery fazy.

04

ETAP 1: ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

Organizacja powinna wdrożyć kompleksowy system zarządzania aktywami informacyjnymi. Kluczowe jest aby organizacja zidentyfikowała wszystkie aktywa informacyjne jakimi dysponuje. Pozwoli to zrozumieć wymagania związane z ich ochroną oraz podjąć właściwe działania zapewniające ich bezpieczeństwo. Etap powinien zakończyć się stworzeniem rejestru aktywów informacyjnych.

Aby zapewnić cyberbezpieczeństwo w organizacji, konieczne jest zidentyfikowanie tego, co rzeczywiście należy chronić. Każda organizacja dysponuje ograniczonymi zasobami, jakie może przeznaczyć na zapewnianie cyberbezpieczeństwa, zatem konieczne jest określenie tego co dla danego podmiotu jest najcenniejsze, co jest istotne w kontekście odpowiedzialności prawnej, a w konsekwencji co należy priorytetowo zabezpieczyć.
Działania prowadzone na tym etapie, przyczynią się także do zrozumienia otoczenia (prawnego, biznesowego, regulacyjnego itd.) w jakim funkcjonuje organizacja – poznania wymagań i dostosowania się do nich.

Efektem końcowym tego etapu jest stworzenie rejestru aktywów. Jest on niezbędny do przeprowadzania dalszych działań związanych zarządzaniem ryzykiem jak i do identyfikacji zakresów odpowiedzialności za zapewnienie odpowiedniego poziomu bezpieczeństwa aktywów. Etap składa się z kilku zadań, które należy wykonać.

05

ETAP 1: ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

Zadanie 1: Identyfikacja aktywów informacyjnych.

Aktywa informacyjne należy rozumieć jako wszystkie zasoby informacyjne mające wartość z punktu widzenia organizacji i jej otoczenia. Aktywami będą nie tylko zasoby podstawowe takie jak bazy danych, dokumenty, pliki, ale także wszystko to co jest z nimi powiązane i na nie wpływa: ludzie, procesy, technologie (więcej w załączniku 1). Aktywa muszą być chronione w całym cyklu ich życia: od momentu ich tworzenia, w trakcie gromadzenia, przechowywania, przetwarzania, przekazywania, aż do momentu zniszczenia. Identyfikacji samych aktywów powinno towarzyszyć określenie dodatkowych danych z nimi związanych m.in.: lokalizacji, formatu, ilości, długość życia itd. Należy pamiętać również o wpływie aktywów na realizację procesów w organizacji. Pozwoli to na bardziej efektywne zarządzanie aktywami i obniżenie poziomu ryzyka .

Zadanie 2: Identyfikacja i przypisanie właściciela dla każdego z aktywów.

Każdy zbiór aktywów powinien mieć przypisanego właściciela. Właściciel jest odpowiedzialny za zarządzanie aktywami, w tym za działania związane z bezpieczeństwem. Zarządzanie aktywami jest procesem, który nie kończy się po jednorazowym zrealizowaniu. Musi być powtarzany i ulepszany w czasie. Dlatego zadaniem właściciela będzie także regularne aktualizowanie działań związanych z aktywami, w tym tych związanych bezpośrednio z zapewnieniem bezpieczeństwa. Wymagana jest stała współpraca pomiędzy właścicielami różnych aktywów w celu utrzymania stabilności funkcjonowania organizacji.

Warto podkreślić, że właściciel jest odpowiedzialny za codzienne zarządzanie aktywami, jednak ostateczną, strategiczną odpowiedzialność prawną, biznesową itd. ponosi kierownictwo organizacji.

06

ETAP 1: ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

Zadanie 3: Określenie wymagań związanych z ochroną aktywów.

Na funkcjonowanie organizacji wpływa wiele czynników zarówno wewnętrznych jak i zewnętrznych. Stanowią one kontekst funkcjonowania podmiotu. Wynikają one między innymi z obowiązków prawnych (np. ochrona danych osobowych), otoczenia biznesowego itp. Analiza kontekstu pozwala zidentyfikować wszystkie dodatkowe wymagania (np. prawne) związane z ochroną aktywów, które należy wdrożyć w życie.

Zadanie 4: Określenie wartości aktywów i ich klasyfikacja.

Celem działania jest poznanie wartości wcześniej zidentyfikowanych aktywów i jasne zakomunikowanie jej wszystkim zainteresowanym podmiotom. Przy dokonywaniu klasyfikacji należy wziąć pod uwagę wewnętrzne i zewnętrzne uwarunkowania organizacji. Podstawowa klasyfikacja może sprowadzać się do opisu np. “poufne” oraz “publiczne”. Dodatkowo, właściciel aktywu może dodać opis skutków utraty poufności, integralności oraz dostępności danego aktywu w zakresie cyberbezpieczeństwa jak i innych wymagań prawnych np. ochrony danych.

07

ETAP 1: ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

Zadanie 5: Identyfikacja obecnie stosowanych zabezpieczeń. Organizacja powinna zidentyfikować zabezpieczenia, które już są stosowane.

Na tym etapie istotne jest ustalenie i udokumentowanie jakie zabezpieczenia już zostały wdrożone i są zastosowane w organizacji. Pozwoli to między innymi lepiej zrozumieć ryzyko, uniknąć duplikowania działań oraz pomoże lepiej zaplanować wdrożenie innych zabezpieczeń. Warto podkreślić, że zabezpieczenia powinny być rozumiane szeroko. Mogą nimi być zarówno procesy, rozwiązania technologiczne, organizacyjne i inne.

Zadanie 6: Stworzenie i utrzymanie rejestru aktywów informacyjnych.

Zadanie to sprowadza się do stworzenia rejestru. Nie jest to jednorazowe działanie. Rejestr powinien być sprawdzany i aktualizowany w ustalonych odstępach czasu oraz zawsze wtedy kiedy wprowadzane są poważniejsze zmiany w organizacji lub gdy miało miejsce jakieś zdarzenie związane z bezpieczeństwem. Incydenty związane z bezpieczeństwem powinny być zarejestrowane w oddzielnym rejestrze.

08

ETAP 2: ZARZĄDZANIE RYZYKIEM

Organizacja powinna wdrożyć proces związany z zarządzaniem ryzykiem. Jednym z ważniejszych elementów procesu jest przeprowadzenie szacowania ryzyka. Szacowanie pozwoli podjąć odpowiednie decyzje związane z zapewnieniem bezpieczeństwa w organizacji.

Głównym celem tego etapu jest przeanalizowanie ryzyk jakie stoją przed organizacją i podjęcie właściwych działań związanych z bezpieczeństwem. Proces powinien być udokumentowany.

Każda organizacja posiada ograniczone zasoby (finansowe, osobowe, rzeczowe itd.) i musi skupić swoje działania na tych ryzykach, które są z punktu widzenia bezpieczeństwa i wymogów prawnych najważniejsze. Szacowanie ryzyka pozwala zrozumieć sytuację i wdrożyć najlepszą strategię postępowania jednocześnie maksymalizując wykorzystanie zasobów organizacji.

Etap podzielony został na 4 fazy, z których każda zawiera kilka zadań, które należy wdrożyć w organizacji.

09

ETAP 2: ZARZĄDZANIE RYZYKIEM

Faza 1: Identyfikowanie ryzyka

Zadanie 1: Identyfikacja zagrożeń, które mogą negatywnie oddziaływać na bezpieczeństwo aktywów.

Organizacja powinna zidentyfikować wszystkie zagrożenia, które mogą negatywnie wpływać na bezpieczeństwo wcześniej zidentyfikowanych aktywów. Organizacja powinna także wskazać źródła zagrożeń. Celem jest tutaj jak najlepsze rozpoznanie, kto lub co oraz w jaki sposób w największym stopniu może zagrozić bezpieczeństwu organizacji. Przykładowa kategoryzacja źródeł zagrożeń w załączniku 2.

Zadanie 2: Identyfikacja podatności na ryzyko.

Podatność jest rozumiana jako słabość aktywów lub stosowanych zabezpieczeń, która może zostać wykorzystana przez zagrożenie. Celem działania jest określenie możliwie wszystkich słabości mogących się zmaterializować w zakresie różnego sposobu lub w różnych warunkach wykorzystywania aktywów. Należy mieć świadomość, że negatywne oddziaływanie na bezpieczeństwo aktywów, może przełożyć się na zakłócanie osiągania celów całej organizacji.

ETAP 2: ZARZĄDZANIE RYZYKIEM

Faza 2: Analiza ryzyka

W celu poprawnego przeprowadzenia procesu jakościowej lub ilościowej analizy ryzyka organizacja musi zbadać dwa elementy: prawdopodobieństwo materializacji wcześniej zidentyfikowanych ryzyk oraz skutki ich wystąpienia. Warto podkreślić, że niemożliwe jest wyeliminowanie wszystkich ryzyk jakie wiążą się z funkcjonowaniem organizacji. Analiza ryzyka pozwala jednak upewnić się, że decyzje związane z działaniami na rzecz bezpieczeństwa wynikają z obiektywnej analizy.

Zadanie 1: Ocena potencjalnych skutków wystąpienia zidentyfikowanych zagrożeń.

W tym zadaniu kluczowe jest aby organizacja oceniła skutki wystąpienia zagrożenia, które będzie miało negatywny wpływ na aktywa informacyjne. Ważne jest uświadomienie, że skutki mogą być wielowymiarowe, mogą dotyczyć wielu obszarów, dlatego istotna jest ich analiza w kontekście możliwych do wystąpienia zdarzeń jakie mogą wygenerować koszty, straty. Są to zdarzenia związane m.in. z:

- z utratą aktywów informacyjnych,
- z nieuprawnionym dostępem do aktywów informacyjnych,
- z nieuprawnioną zmianą aktywów informacyjnych.

Wskazane powyżej zdarzenia powinny być podstawą do oszacowania skutków dotyczących np.:

- kosztów związanych z przestojem pracy, świadczenia usług,
- kosztów związanych z dochodzeniami dotyczącymi incydentów (włączając w to koszty działań związanych z informatyką śledczą, usługami doradczymi itd.),
- kosztów związanych z zarządzaniem kryzysowym – np. koszty dotyczące zarządzania incydentem, z informowaniem klientów o stratach i negatywnych skutkach itd.,
- kosztów związanych z prawnymi i regulacyjnymi sankcjami,
- kosztów związanych z utraconymi szansami, takimi jak uszkodzona reputacja, utraceni potencjalni.

ETAP 2: ZARZĄDZANIE RYZYKIEM

Faza 2: Analiza ryzyka

Zadanie 2: Ocena prawdopodobieństwa wystąpienia zagrożenia.

Po określeniu skutków następnym krokiem powinna być analiza prawdopodobieństwa wystąpienia danego zagrożenia. Na tym etapie należy uwzględnić wcześniej wskazane, elementy: źródła zagrożeń, podatności, istniejące zabezpieczenia, ich skuteczność popartą wiedzą ich faktycznego funkcjonowania itd. Oceniając prawdopodobieństwo organizacja powinna czerpać informacje z różnych źródeł na przykład: z doświadczenia własnego i swoich pracowników, z wydarzeń historycznych, ze statystyki, z raportów eksperckich itd.

Zadanie 3: Określenie akceptowalnego poziomu ryzyka.

Organizacja powinna określić akceptowalne poziomy ryzyka. Pozwolą one ocenić, z którymi ryzykami i na jakim poziomie organizacja jest w stanie funkcjonować. Ustalenie akceptowalnych poziomów ryzyka pozwoli potem porównać je z poziomami ryzyka wynikającymi z analizy ryzyka. Przy ustalaniu akceptowalnego poziomu ryzyka należy wziąć pod uwagę wcześniej przyjętą klasyfikację, zbudowaną w oparciu o wartości przypisane poszczególnym aktywom. To kierownictwo organizacji powinno zadecydować jaki poziom ryzyka zgodzi się zaakceptować. W procesie tym kierownictwo wspierać powinni właściciele aktywów. Działania podejmowane w tym zadaniu będą istotnie wpływały na późniejszy etap, kiedy organizacja podejmować będzie decyzję dotyczące postępowania z ryzykiem.

ETAP 2: ZARZĄDZANIE RYZYKIEM

Faza 3: Ocena analizowanego ryzyka.

Porównanie wyników analizy ryzyka z wcześniej określonymi akceptowalnymi poziomami ryzyka.

Porównanie wyników analizy ryzyka z wcześniej określonymi akceptowalnymi poziomami ryzyka.

W sytuacji kiedy wynik analizy ryzyka (faza 2) jest niższy lub równy akceptowalnemu poziomowi ryzyka przypisanemu do aktywu informacyjnego, organizacja może zaakceptować ryzyko. Decyzja ta powinna zostać udokumentowana oraz potwierdzona podpisem kierownictwa organizacji. Następnie, należy regularnie przeglądać ryzyko i upewniać się, że pozostaje na akceptowalnym poziomie.

W sytuacji gdy jednak poziom ryzyka będzie wyższy, organizacja powinna podjąć decyzję o podjęciu stosownych działań zgodnie z ustaloną strategią postępowania.

ETAP 3: WYBÓR ZABEZPIECZEŃ I ICH IMPLEMENTACJA

Organizacja powinna wybrać i wdrożyć adekwatne zabezpieczenia które podnosząc poziom bezpieczeństwa redukują stopień zidentyfikowanych ryzyk do akceptowalnego poziomu.

Istnieją cztery główne (nie jedyne) kategorie zabezpieczeń przyczyniających się do zwiększania bezpieczeństwa:

- bezpieczeństwo osobowe (w tym szkolenia),
- bezpieczeństwo techniczne,
- bezpieczeństwo fizyczne,
- bezpieczeństwo organizacyjne.

Wszystkie rodzaje zabezpieczeń mają za zadanie między innymi przeciwdziałać incydentom, pomóc w ich wykrywaniu i minimalizować ewentualne skutki.

Opierając się na wynikach analizy ryzyka, właściciel aktywu informacyjnego (jeśli potrzeba w konsultacji z innymi podmiotami) powinien zdecydować, które zabezpieczenia powinny zostać zastosowane. Implementacja zabezpieczeń ma doprowadzić do obniżenia poziomu ryzyka do poziomu akceptowalnego.

Decydując się na konkretne zabezpieczenia i wdrażając je, organizacja powinna mieć na uwadze, że kluczem dla osiągania jej celów jest utrzymanie ciągłości biznesowej.

ETAP 4: TESTOWANIE BEZPIECZEŃSTWA, MONITORING, AUDYT, CIĄGŁE DOSKONALENIE

Aby nadążyć za nieustannie zmieniającymi się czynnikami wpływającymi na bezpieczeństwo, organizacja powinna regularnie podnosić, utrzymywać i aktualizować działania nakierowane na jego zapewnienie.

Wdrażanie działań związanych z bezpieczeństwem nigdy nie może być traktowane jako działania jednorazowe. Jest to proces, który powinien być monitorowany i powtarzany w regularnych odstępach czasu. Kluczowe elementy procesu utrzymania cyberbezpieczeństwa, (takie jak szacowanie ryzyka) powinny być sprawdzane, aktualizowane regularnie oraz zawsze kiedy zachodzą poważne zmiany w organizacji, lub doszło do poważnych incydentów oraz zdarzeń związanych z bezpieczeństwem.

Dodatkowo organizacja powinna przeprowadzać testy i audyty bezpieczeństwa. Ważną rolę w tych procesach pełni właściciel aktywów, jako osoba wspomagająca kierownictwo organizacji w nadzorowaniu, prawidłowej realizacji wszystkich wyżej wymienionych działań.

Działania podejmowane na etapie 4 powinny być dokumentowane.

15

ZAŁĄCZNIKI

Załącznik 1: Przykłady aktywów informacyjnych

- Informacje: bazy danych, dokumenty i pliki danych (dane klienta, dane finansowe, dane pracowników, informacje o produktach, umowy, plany, dokumentacja systemu, informacje o badaniach, materiały szkoleniowe, procedury operacyjne itp.), zapisy audio i video, klucze szyfrowania i certyfikaty, dane dotyczące pracy i funkcjonowania oprogramowania, systemów jak i aktywności osób, hasła i identyfikatory.
- Oprogramowanie: aplikacje, oprogramowanie systemowe, dane konfiguracyjne, zabezpieczenia softwarowe itp.
- Procesy: procesy księgowe, procesy HR, procesy produkcyjne itp.
- Zasoby fizyczne: sprzęt komputerowy, urządzenia telekomunikacyjne, nośniki, zabezpieczenia fizyczne itp.
- Usługi: usługi przetwarzania i przesyłania, zasilanie, niszczenie danych itp.
- Ludzie: pracownicy, kierownictwo, osoby trzecie itp.

Załącznik 2: Przykładowa kategoryzacja źródeł zagrożeń

- Wewnętrzne (pracownicy posiadający nadmiarowe uprawnienia, pracownicy nieprzeszkoleni lub posiadający niską świadomość bezpieczeństwa, pracownicy posiadający specjalne uprawnienia, niesprawne lub nieskuteczne zabezpieczenia).
- Wrogie podmioty (np. hakerzy, haktywiści, przestępcy i zorganizowane grupy przestępcze, państwa realizujące wrogie działania w cyberprzestrzeni, terroryści).
- Zagrożenia pochodzące ze środowiska naturalnego (np. pożar, powódź, trzęsienie ziemi).
- Zagrożenia biznesowe (brak dostaw mediów, awaria sprzętu, zagrożenia związane z łańcuchem dostaw, pracownicy).

16

ZAŁĄCZNIKI

Załącznik 3: Kluczowe zasady wdrożenia standardu

- Standard musi być traktowany jako integralny element strategicznego funkcjonowania organizacji. Działania na rzecz cyberbezpieczeństwa powinny być ściśle powiązane z misją, celami oraz procesami realizowanymi w organizacji.
- Cyberbezpieczeństwo powinno być traktowane jako element całościowego systemu bezpieczeństwa organizacji.
- Warunkiem koniecznym do efektywnego i skutecznego wdrożenia standardu jest uzyskanie wsparcia od najwyższych szczebli zarządzających w organizacji.
- Kluczowym elementem jest ciągłe uświadamianie i komunikowanie celów i obowiązków związanych z cyberbezpieczeństwem wszystkim zaangażowanym podmiotom, zgodnie z ich obszarem działań i odpowiedzialności.
- Cyberbezpieczeństwo jest strategicznym aspektem funkcjonowania organizacji. Dlatego działania, które organizacja zdecyduje się wdrażać w tym obszarze, muszą mieć zapewniony właściwy budżet i zasoby kompetencyjne. Poziom cyberbezpieczeństwa powinien być między innymi wypadkową wyników procesu szacowania ryzyka określonego zgodnie z otoczeniem i kontekstem działania organizacji.
- Wszystkie działania podejmowane w ramach wdrażania standardu nie mogą być traktowane jako jednorazowe zadanie do zrealizowania, ale jako ciągły proces, nieustannie doskonalący i modyfikujący stosowane rozwiązania. Kwestie związane z cyberbezpieczeństwem ewoluują wraz ze zmianą celów i kontekstu funkcjonowania organizacji oraz specyfiką zagrożeń.
- Działania zawarte w standardzie są zbudowane na podejściu opartym na ryzyku. Taki typ postępowania pomaga rozwiązać problem ograniczonych zasobów jakimi dysponuje organizacja. Wynika to z faktu, że organizacja jest w stanie zidentyfikować i zabezpieczyć najcenniejsze aktywa, biorąc pod uwagę ryzyko jakie ich dotyczy.

POLSKA PLATFORMA
BEZPIECZEŃSTWA WEWNĘTRZNEGO

Polska Platforma Bezpieczeństwa Wewnętrznego

ul. Słowackiego 17/11
60-822 Poznań
www.ppbw.pl
tel.: (61) 663 02 21
e-mail: sekretariat@ppbw.pl

Fundusze Europejskie Inteligentny Rozwój

Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Projekt pt.: „Cyberbezpieczeństwo – standard PPBW dla MŚP i instytucji publicznych" współfinansowany ze środków Unii Europejskiej.