KLASYFIKACJA DANYCH

KLASYFIKACJA DANYCH JEST ELEMENTEM STANDARDU CYBERBEZPIECZEŃSTWA PPBW DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW ORAZ INSTYTUCJI PUBLICZNYCH, OPRACOWANEGO PRZEZ POLSKĄ PLATFORMĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO.

SPIS TREŚCI

1. CZYM JEST I DO CZEGO SŁUŻY KLASYFIKACJA INFORMACJI?..... 03
2. WSKAZÓWKI DOTYCZĄCE PRZYGOTOWANIA KLASYFIKACJI..... 04
3. JAKIE KROKI PODJĄĆ ABY STWORZYĆ KLASYFIKACJE..... 06
4. PRZYKŁADOWA KLASYFIKACJA
   - **4.1** Informacje ściśle chronione..... 07
   - **4.2** Informacje wyłacznie do użytku wewnętrznego..... 08
   - **4.3** Informacje publicznie dostępne..... 09
5. WIĘCEJ IFORMACJI NT. KLASYFIKACJI..... 10

03

CZYM JEST I DO CZEGO SŁUŻY KLASYFIKACJA INFORMACJI?

- Klasyfikacja informacji to grupowanie zasobów/aktywów informacyjnych według kryteriów związanych z ich wagą dla organizacji oraz otoczenia.

- Pozwala ona zidentyfikować i oznaczyć najważniejsze zasoby/aktywa, a tym samym zapewnić skuteczną ochronę. Wynika to z tego, że dla każdej kategorii określone zostają zabezpieczenia i podstawowe metody postępowania.

- Dobrze wykonana klasyfikacja zasobów/aktywów pozwala wszystkim pracownikom (oraz zewnętrznym interesariuszom) właściwie obchodzić się z informacjami – między innymi stosować adekwatne środki ochrony.

- Klasyfikacja informacji pozwala także lepiej przeprowadzić proces oceny ryzyka.

04

WSKAZÓWKI DOTYCZĄCE PRZYGOTOWANIA KLASYFIKACJI

- Nie ma jednej uniwersalnej metody opracowania klasyfikacji informacji, która pasowałaby do wszystkich typów podmiotów.

- Biorąc pod uwagę specyficzne uwarunkowania funkcjonowania każdej organizacji, każdy podmiot powinien stworzyć swój własny system klasyfikacji lub dostosować istniejące wzorce.

UWAGA

Istnieją regulacje prawne, które narzucają reguły klasyfikacji aktywów/zasobów informacyjnych oraz wskazują bardzo konkretne mechanizmy zapewniania bezpieczeństwa. Przykładem może być ochrona informacji niejawnych. Oczywiście wtedy organizacja zobowiązana jest podążać za wytycznymi prawnymi. Dlatego tworzenie klasyfikacji powinno dotyczyć aktywów/zasobów, których nie dotyczą przepisy określające konkretne działania związane z bezpieczeństwem. Klasyfikacja powinna uzupełniać (nie zastępować), te wynikające z wymagań prawnych.

05

WSKAZÓWKI DOTYCZĄCE PRZYGOTOWANIA KLASYFIKACJI

- Przy stosowaniu określonego nazewnictwa przy projektowaniu systemu klasyfikacji, należy unikać terminów, które mogą być mylące – np. nie należy stosować nazwy „ściśle tajne" (stosowanej w systemie ochrony informacji niejawnych) wtedy kiedy organizacja nie przetwarza prawnie chronionych informacji niejawnych.

- Poza wzięciem pod uwagę wymagań wynikających z powszechnych regulacji prawnych, przy budowaniu klasyfikacji organizacja powinna brać pod uwagę inne wymagania wynikające np. ze zobowiązań umownych dotyczących ochrony informacji zgodnie ze specyfikacjami klienta lub partnera biznesowego.

- Klasyfikacja musi być zrozumiała dla wszystkich użytkowników, nie nazbyt skomplikowana, tak aby wszyscy pracownicy łatwo umieli ją zastosować. Jednocześnie nie powinna być zbyt ogólna.

- Tworzenie systemu klasyfikacji jest ciągłym procesem, który powinien być udoskonalany w czasie.

- Klasyfikacja powinna być budowana z uwzględnieniem trzech głównych atrybutów bezpieczeństwa:

    - poufności – ochrony aktywów/zasobów informacyjnych przed podmiotami, które nie powinny mieć do nich dostępu,
    - integralności – ochrony aktywów/zasobów informacyjnych przed nieuprawnionymi bądź losowymi zmianami, uszkodzeniami,
    - dostępności – zapewnienia, że uprawniona osoba będzie mogła mieć dostęp do danego zasobu/aktywu informacyjnego wtedy gdy będzie to potrzebne.

06

JAKIE KROKI PODJĄĆ ABY STWORZYĆ KLASYFIKACJE

KROK 1

UŻYJ REJESTRU ZINWENTARTYZOWANYCH AKTYWÓW/ZASOBÓW INFORMACYJNYCH
(ETAP 1 STANDADRU PPBW)

KROK 2

OKREŚL KATEGORIE DLA GRUP AKTYWÓW/ZASOBÓW INFORMACYJNYCH WYSTĘPUJĄCYCH W OGRANIZACJI

KROK 3

OKREŚL ŚRODKI ZWIĄZANE Z BEZPIECZEŃSTWEM I SPOSOBY POSTĘPOWANIA Z AKTYWAMI/ZASOBAMI PRZYPISANYCH DO KAŻDEJ KATEGORII

KROK 4

PRZYPISZ KATEGORIE DO WCZEŚNIEJ ZIDENTYFIKTOWANYCH ZASOBÓW
(OZNACZ JE)

07 PRZYKŁADOWA KLASYFIKACJA

Poniżej zastosowano przykładową, trzypoziomową klasyfikację informacji wraz z ilustracją jaki zasób/aktyw mógłby mieścić się w poszczególnych kategoriach.

Klasyfikacja zawiera także przykładowe wymagania dotyczące postępowania związanego z ochroną.

KATEGORIA: INFORMACJE ŚCIŚLE CHRONIONE

OPIS/WYJAŚNIENIE

Nieuprawniony dostęp do aktywów/zasobów informacyjnych z tej kategorii (szczególnie przez podmioty zewnętrzne), brak dostępu do nich wtedy kiedy istnieje potrzeba (np. z powodu zniszczenia), nieuprawniona ich zmiana mogłoby przynieść bardzo negatywne skutki dla organizacji lub/i dla podmiotów z nią współpracujących (np. klientów, partnerów biznesowych).

Bardzo negatywne skutki mogą dotyczyć np. znacznych strat finansowych, wizerunkowych, a nawet stanowić zagrożenie dla bezpieczeństwa niektórych osób.

Naruszenie bezpieczeństwa aktywów/zasobów informacyjnych, stanowić może naruszenie wymagań prawnych lub zobowiązań umownych.

PRZYKŁAD

Dane związane z bezpieczeństwem (np. dane do logowania, hasła, dane konfiguracyjne, informacje dotyczące incydentów).

Specjalne kategorie danych osobowych (np. dotyczące zdrowia, sytuacji finansowej danej osoby, dane biometryczne).

Dane biznesowe i finansowe:
(np. strategie negocjacyjne, tajne plany projektów, dane dot. kart kredytowych, dane księgowe np. wynagrodzenia, rozliczenia podatkowe, dane dotyczące przetargów).

Poufne umowy i warunki współpracy z klientami i kontrahentami.

OCHRONA

Dostęp: wyłącznie osoby (mogą to być kategorie osób/funkcje) z pisemnym upoważnieniem Zarządu.

Uwierzytelnienie: dwustopniowa weryfikacja użytkownika.

Przesyłanie: wyłącznie osobom lub podmiotom znajdującym się na liście zatwierdzonej przez Zarząd.

Szyfrowanie: informacje mogą być przesyłane wyłącznie przy użyciu szyfrowanych kanałów transmisyjnych.

Backup: codzienny

Niszczenie: w sposób uniemożliwiający odzyskanie.

08

PRZYKŁADOWA KLASYFIKACJA

KATEGORIA: INFORMACJE WYŁĄCZNIE DO UŻYTKU WEWNĘTRZNEGO

OPIS/WYJAŚNIENIE

Aktywa/zasoby informacyjne wykorzystywane powinny być wyłącznie na użytek wewnętrzny organizacji i na jej potrzeby.

Są to nie newralgiczne zasoby/aktywa związane z codziennym funkcjonowaniem organizacji, ale równocześnie takie, którym powinny być zapewnione wybrane metody ochrony.

Problemy związane z poufnością, dostępnością i integralnością mogłyby zakłócić efektywne funkcjonowanie organizacji.

Bez pozwolenia nie powinny być ujawniane nikomu spoza organizacji.

PRZYKŁAD

- dane osobowe (poza specjalnymi kategoriami danych osobowych),
- wewnętrzne regulaminy i wewnętrzne polityki,
- notatki służbowe,
- procedury,
- szablony umów,
- bazy klientów,
- narzędzia do zarządzaniem zadaniami.

OCHRONA

Dostęp: dostęp dla osoby (mogą to być kategorie osób/funkcje) zatwierdzony przez właściciela zasobu.

Uwierzytelnienie: dwustopniowa weryfikacja użytkownika.

Przesyłanie: wyłącznie osobom lub podmiotom znajdującym się na liście zatwierdzonej przez właściciela zasobu.

Szyfrowanie: wymagane przy wysyłaniu do zewnętrznych podmiotów.

Backup: cotygodniowy

Niszczenie: w sposób uniemożliwiający odzyskanie.

09

PRZYKŁADOWA KLASYFIKACJA

KATEGORIA: INFORMACJE PUBLICZNIE DOSTĘPNE

OPIS/WYJAŚNIENIE

Aktywa/zasoby informacyjne, które bez ograniczeń mogą być (lub w niektórych przypadkach powinny być) udostępniane publicznie i dystrybuowane.

PRZYKŁAD

- reklama,
- informacje promocyjne firmy,
- oficjalne cenniki,
- strona internetowa.

OCHRONA

Dostęp: nieograniczony

Uwierzytelnienie: brak

Przesyłanie: dowolne

Szyfrowanie: brak

Backup: raz na miesiąc

Niszczenie: bez szczególnych wymagań

10

WIĘCEJ INFORMACJI NA TEMAT KLASYFIKACJI:

S. Fowler, Information Classification -Who, Why and How, SANS Institute, 2019.

ISO27k Forum at www.ISO27001security.com.

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: standard-cyber@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.