Bezpieczeństwo infrastruktury krytycznej i systemów sterowania przemysłowego IoT - LAB 5 Zarządzanie bezpieczeństwem informacji

GR

Imiona i nazwiska członków grupy:

Zadanie numer 1

Krok 1: Proszę określić misję funkcjonowania podmiotu (po co podmiot działa) – misja może być wyrażona przez cele, które poprzez swoje funkcjonowanie chce osiągać podmiot. (*Np. Misją funkcjonowania placówki zdrowia jest leczenie pacjentów, dbanie o ich komfort przy dochodzeniu do zdrowia. Powiązanymi z tymi celami będą np. skuteczne leczenie, opieka itd.*).

Podmioty do wyboru:

- Elektrownia
- Lotnisko
- Wodociągi
- Itp.

Krok 2: Proszę zidentyfikować 10 procesów realizowanych w analizowanym podmiocie i wpisać je do poniższej tabelki. (*w czytanym przez Państwa tekście M. Ossowskiego wskazano podział na procesy „podstawowe i pomocnicze", „procesy operacyjne i procesy wspomagające" – wychodząc z tego podejścia proszę szeroko myśleć o identyfikacji procesów).

Następnie proszę zaproponować właściciela procesu – czyli podmiot, osobę, która będzie w firmie odpowiedzialna za dany proces.

Lp.	PROCES (NAZWA & KRÓTKI OPIS)	WŁAŚCICIEL
1		
2		
3		
4		
5		
6		

7		
8		
9		
10		

Krok 3: Teraz, proszę skupić się wyłącznie na wybranych 4 procesach. Wykorzystując metodę „burzy mózgów” proszę opisać/rozrysować działania, jakie należy podjąć aby zrealizować dany proces (można rozrysować sobie proces na kartce / innym środowisku do rysowania).

Krok 4: Następnie proszę o wypisanie wszystkich możliwych zasobów/aktywów informacyjnych wykorzystywanych w ramach każdego z 4 realizowanych procesów. Proszę wypisać zarówno aktywa/zasoby podstawowe jak i wspierające.

[przykład: aktywa podstawowe – CV kandydata do pracy; aktywa wspierające – Folder na Google Drive gdzie umieszczane są CV].

[Proszę pamiętać o tym, że aktywa należy rozumieć szeroko].

Proces 1

Lp.	AKTYWA
1	

Proces 2

Lp.	AKTYWA
1	Komputer

Proces 3

Lp.	AKTYWA
1	

Proces 4

Lp.	AKTYWA
1	

Krok 5: Za pomocą poniższej macierzy proszę o określenie związku pomiędzy aktywami/zasobami podstawowymi a wspierającymi. Celem jest zidentyfikowanie, które zasoby/aktywa podstawowe wykorzystują jakie zasoby /aktywa wspierające. Tabelka jest poglądowa proszę ją zmodyfikować odpowiednio do swojego scenariusza.

AKTYWA PODSTAWOWE	TBD	TBD	TBD	Dane logowania	Umowy i faktury z ISP	Umowy zw z energetyką	Umowy zw z pracodawstwem
AKTYWA WSPIERAJĄCE							
TBD							
TBD							
TBD							
Telefon							
Pokoje							
Niszczarka							
Dysk							
Stalowe drzwi							
Router							
Konta w mediach społecznościowych							
Drukarka							
Poczta							
Ludzie z działu marketingu							
Zabezpieczenia ppoż							
Pracownicy							
Profile bookingowe							
Infrastruktura sieciowa							
Infrastruktura energetyczna							

Krok 6. Proszę ocenić wartość wcześniej zidentyfikowanych aktywów/zasobów podstawowych biorąc pod uwagę kontekst funkcjonowania podmiotu w tym np. uregulowania prawne.

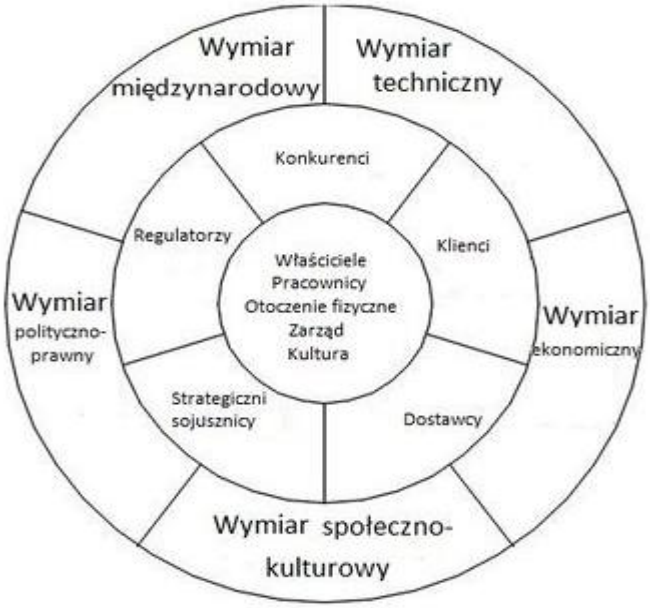
[Wskazówka: określając wartość zasobów proszę wziąć pod uwagę cele funkcjonowania firmy].

AKTYWA PODSTAWOWE	WARTOŚĆ
	Publicznie dostępne
	Do użytku wewnętrznego
	Ściśle chronione

Krok 7: Proszę zastanowić się nad otoczeniem zewnętrznym firmy – z jakimi podmiotami firma wchodzić będzie w interakcje.

Definiujemy otoczenie bliższe:

Lp.	Interesariusze
1	



Elementy otoczenia organizacji,źródło: R.W.Griffin

Zadanie numer 2 – Ocena Ryzyka

Krok 1: Proszę wrócić do 4 wybranych wcześniej procesów i zidentyfikować maksymalnie dużo zagrożeń, które mogą wpłynąć negatywnie ich przebieg i na wykorzystywane do ich realizacji aktywa (na integralność, poufność, dostępność). Proszę być kreatywnym i wskazać możliwie dużo zdywersyfikowanych źródeł zagrożeń (np. związanych z obszarem osobowym, technologicznym, fizycznym itd.). Scenariusze funkcjonowania podmiotów mają być źródłem inspiracji, należy się nimi posiłkować, ale nie traktować jako wyczerpującego materiału ograniczającego w zadaniu. Proszę także brać pod uwagę wcześniej wskazane informacje jak np. to z jakimi interesariuszami wchodzimy w interakcje.

Krok 2: Proszę wybrać 10 zidentyfikowanych zagrożeń i dokonać oceny ryzyka. Wybór konkretnych wartości w ocenie powinien być udokumentowany i wyjaśniony w postaci odpowiedniego komentarza.

Uwaga! Przy ocenie podatności proszę wykazać się kreatywnością i dokonać pewnych teoretycznych założeń (jak również informacji ze scenariusza). Wybór także proszę uzasadnić umieszczając konkretny komentarz.
Np. podatność dla laptopa pracownika oceniona będzie wysoko bowiem zakładamy, że nie ma na nim antywirusa, ani innego zabezpieczenia.
Scenariusze funkcjonowania podmiotów mają być źródłem inspiracji, należy się nimi posiłkować, ale nie traktować jako wyczerpującego materiału ograniczającego w zadaniu

Krok 3: Wynik oceny ryzyka proszę porównać ze skalą poniżej. Tam gdzie ryzyko jest nieakceptowalne proszę zaproponować strategię dalszego działania.

Skala oceny ryzyka			
prawdopodobieństwo wystąpienia/ciężkość następstw	**MAŁA**	**ŚREDNIA**	**DUŻA**
MAŁO PROAWDOPODOBNE	Bardzo małe ryzyko	Małe ryzyko	Średnie ryzyko
PRAWDOPODOBNE	Małe ryzyko	Średnie ryzyko	Duże ryzyko
WYSOCE PRAWDOPODOBNE	Średnie ryzyko	Duże ryzyko	Bardzo duże ryzyko

Zadanie numer 3 – Polityki

Zdefiniować politykę bezpieczeństwa informacji opisywanego podmiotu.

Zadanie numer 4 - Audyt

Zdefiniować jak można przeprowadzić audyt opisywanego podmiotu.