Bezpieczeństwo infrastruktury lokalnej

RCB
Rządowe Centrum Bezpieczeństwa

Witold SKOMRA
Doradca

Materiały wykorzystane w prezentacji:

- Zawiła-Niedźwiecki J.[2013], Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji, edu-Libri;
- Skomra W. (red.) [2015], Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego Rzeczypospolitej Polskiej, SGSP, Warszawa;
- Skomra W. [2018],Panowanie nad ryzykiem w ramach publicznego zarządzania kryzysowego.

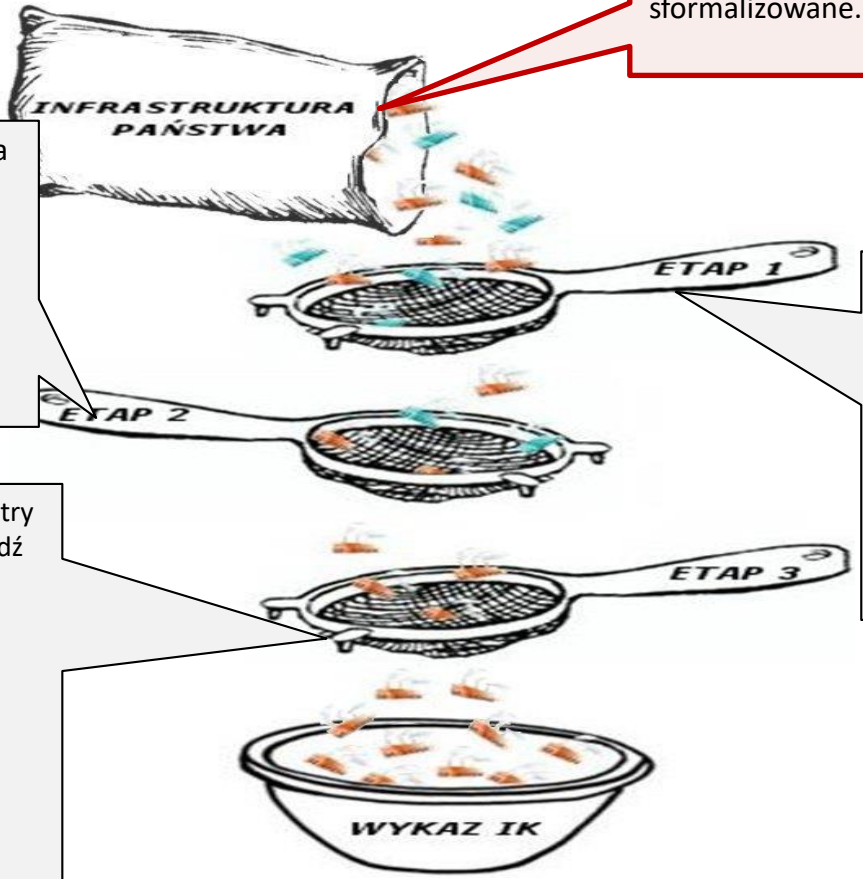
Podstawy prawne:

1. Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.
2. Dyrektywa unijna 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych.
3. Projekt nowelizacji ustawy o zarządzaniu kryzysowym.

Jak jest teraz

Typowanie obiektu „podejrzewanego” o pełnienie roli kluczowej nie jest sformalizowane.

definicja IK – czy pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej,
a także instytucji i przedsiębiorców

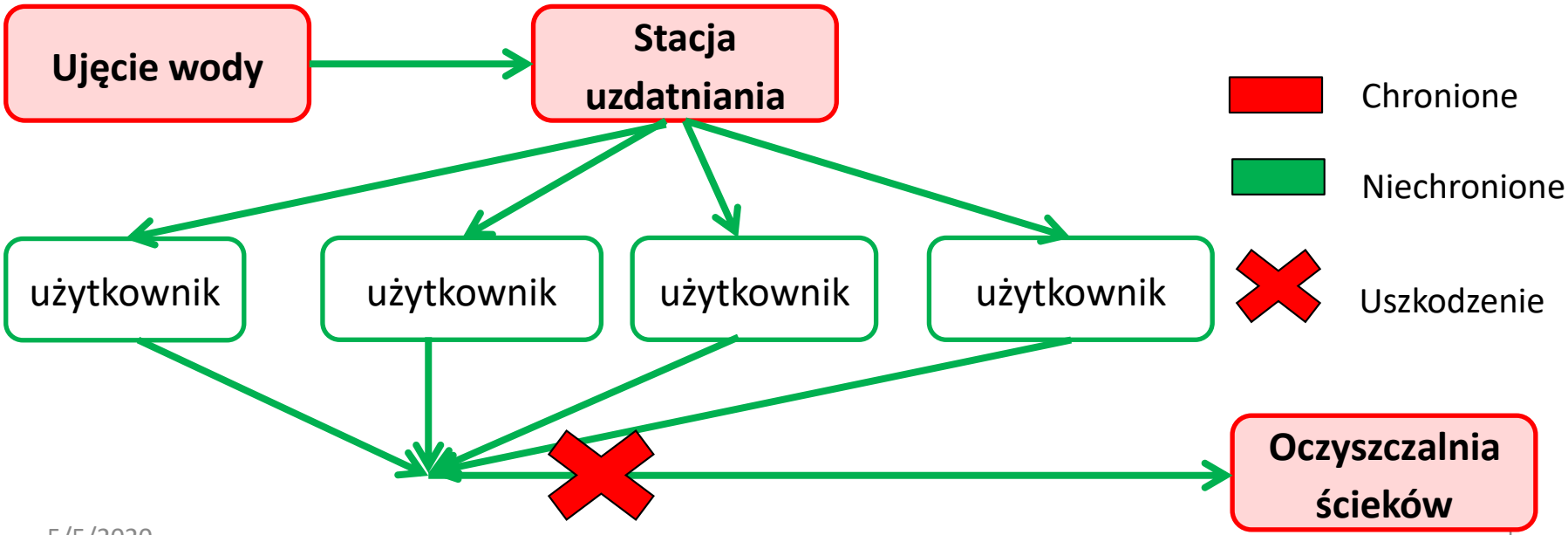


kryteria systemowe – charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do infrastruktury krytycznej. Kryteria te przedstawione są dla każdego z systemów IK

kryteria przekrojowe – opisujące parametry odnoszące się do skutków zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria przekrojowe obejmują:
ofiary w ludziach,
skutki finansowe,
konieczność ewakuacji,
utratę usługi,
czas odbudowy,
efekt międzynarodowy,
unikatowość

Wady podejścia obiektowego – chronimy obiekty zamiast usług

Typowy system zaopatrzenia w wodę

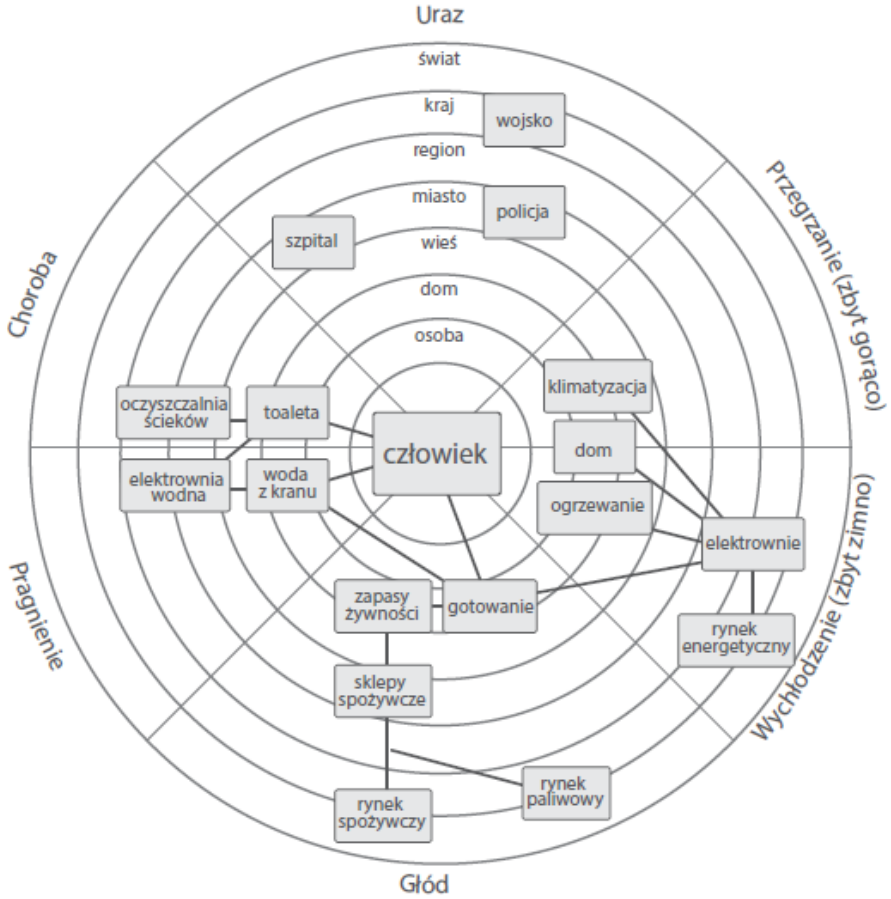


Zidentyfikowane „wady”

1. Nieuwzględnienie niektórych elementów, wchodzących w skład systemów IK, a mających wpływ na świadczenie usług (obiekty są chronione, ale usługa nie funkcjonuje).
2. Niespójność z postanowieniami Dyrektywy NIS i ustawą o Krajowym Systemie Cyberbezpieczeństwa.
3. Brak możliwości zastosowania do „krytycznych” obiektów w odniesieniu do infrastruktury lokalnej.
4. Kryteria przekrojowe nieprzystające do specyfiki niektórych systemów IK.

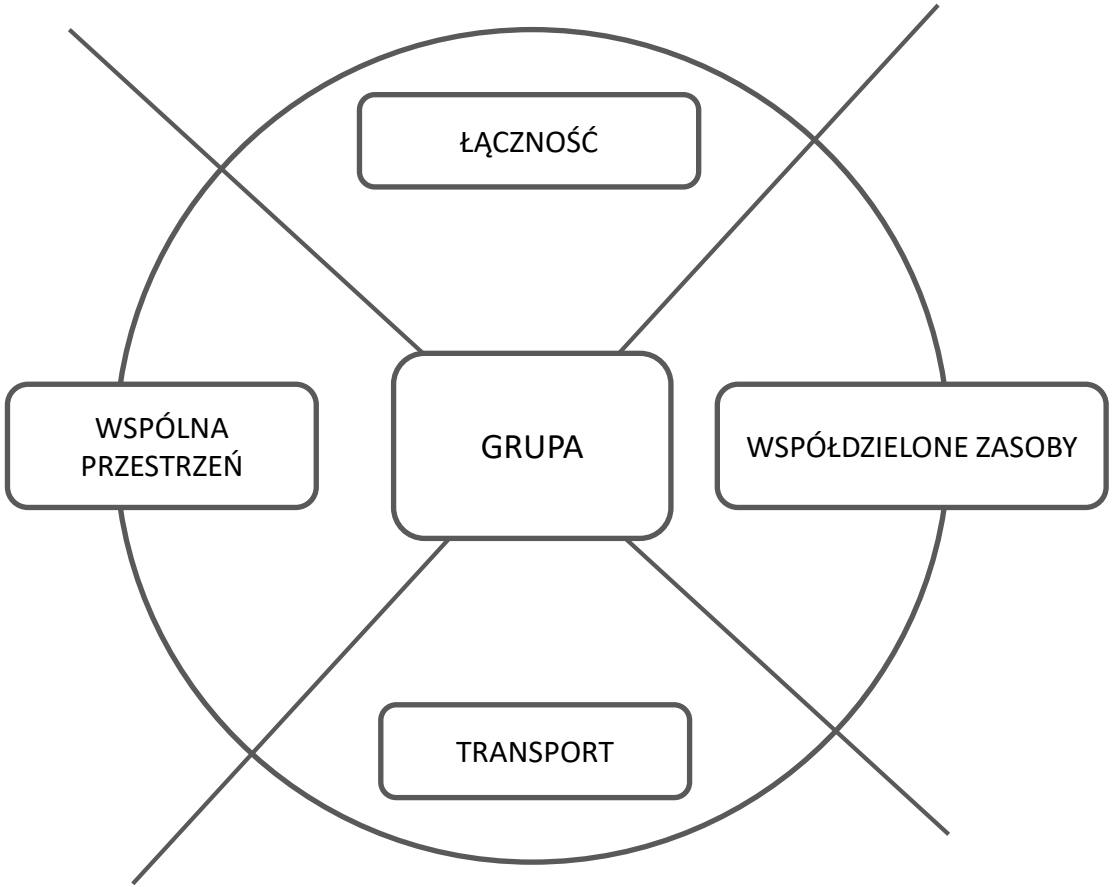
Identyfikacja usług kluczowych

Pierwsza perspektywa – pojedynczy człowiek



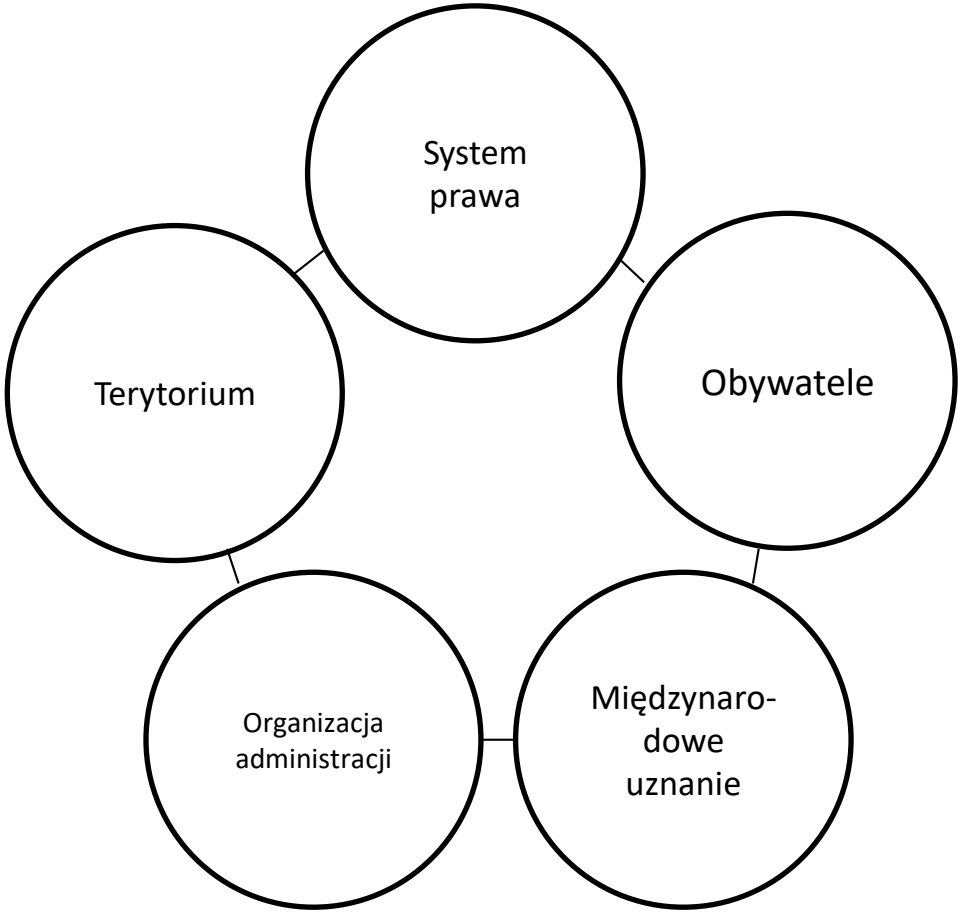
M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe*

Perspektywa druga – grupa



M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe*

Perspektywa trzecia – państwo



M. Bennett, V. Gupta, *Dealing in Security understanding vital services and how they keep you safe*

Perspektywa trzecia – państwo. Przykłady funkcji kluczowych

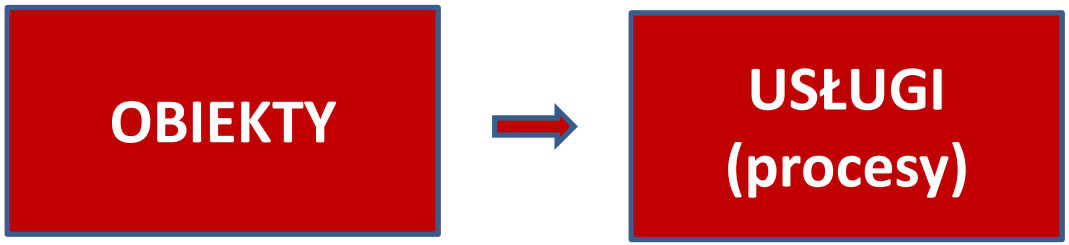
Sys. prawa	• Trybunał Konstytucyjny
Obywatele	• Ewidencja obywateli
Uznanie międzynarodowe	• Demokratyczne wybory
Administracja	• Obsługa PRM, Prezydenta, Sejmu i Senatu
Terytorium	• Ochrona granic.

Perspektywa trzecia – państwo. Nowe podejście w USA

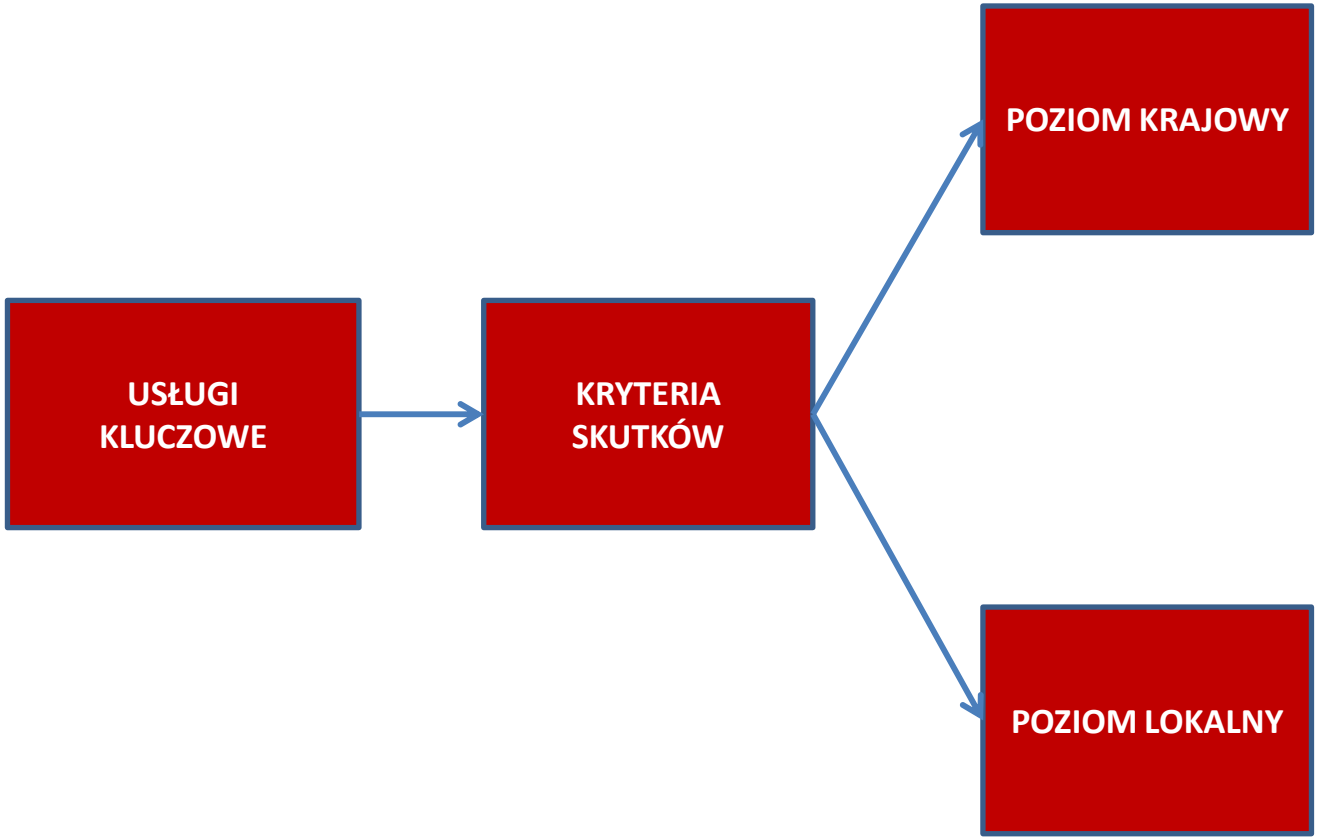
National Critical Functions Set

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access, and Connection Services ▪ Provide Positioning, Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services	▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit	▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government ▪ Perform Cyber Incident Management Capabilities ▪ Prepare for and Manage Emergencies	▪ Exploration and Extraction Of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials

Źródło: The Cybersecurity and Infrastructure Security Agency USA (CISA)
https://www.dhs.gov/cisa/national-critical-functions-overview


OBIEKTY
USŁUGI
(procesy)

Nowy pomysł na identyfikację IK



Priorytety NPOIK 2021 - propozycje

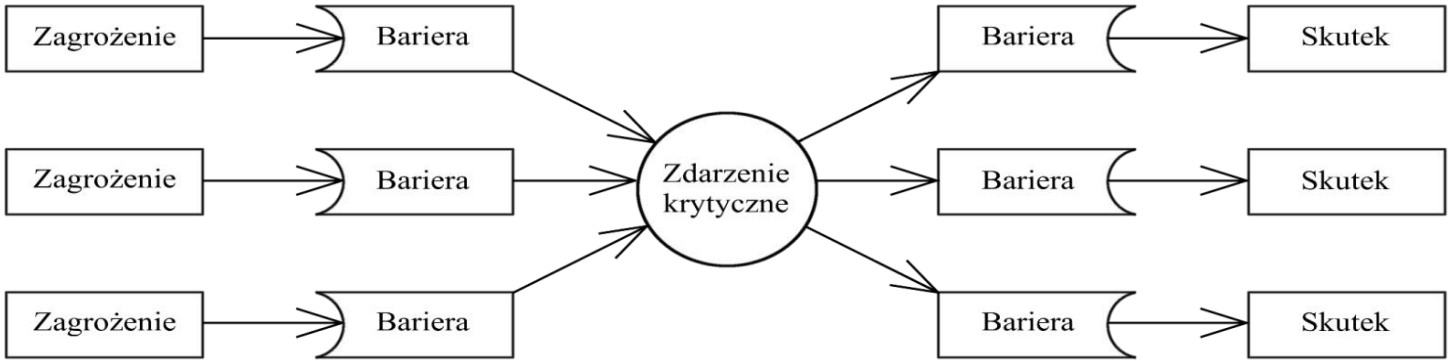
1. Przejście z ochrony obiektów na ochronę usług z podziałem na usługi o znaczeniu krajowym i lokalnym.
2. Uspójnienie procesu wyłaniania usług kluczowych w myśl ustawy o Krajowym Systemie Cyberbezpieczeństwa i ustawy o Zarządzaniu Kryzysowym.
3. Rozszerzenie zarządzania bezpieczeństwem na kompleksowe zarządzanie ryzykiem

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

Dyrektywa ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa **sieci i systemów informatycznych** w Unii, aby poprawić funkcjonowanie rynku wewnętrznego.

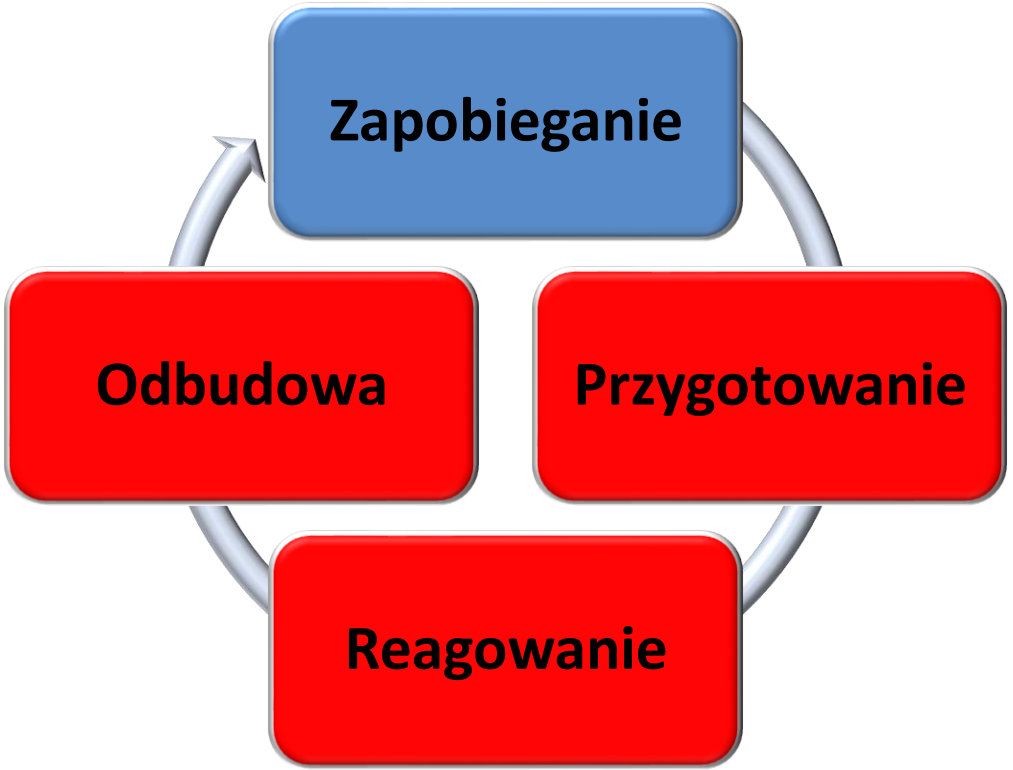
Priorytet nr 3. Rozszerzenie zarządzania bezpieczeństwem na kompleksowe zarządzanie ryzykiem

Zarządzanie ryzykiem → **Zarządzanie bezpieczeństwem** → **Zarządzanie ciągłością**



Analiza metodą Bowtie. Drzewo błędów – drzewo zdarzeń

Priorytet nr 3 – Rozszerzenie zarządzania bezpieczeństwem na kompleksowe zarządzanie ryzykiem



	Zarządzanie ryzykiem	Bariera	Zarządzanie ciągłością			Ewaluacja
	Zapobieganie		Przygotowanie	Reagowanie	Odtwarzanie	
Plany ciągłości działania i odtwarzania	BIA + Bowtie Zmapowane procesy. Analiza ryzyka.	Świadomość ryzyka w organizacji	Plan Ciągłości Działania BCP	Przygotowany i przeszkolony zespół reagowania kryzysowego	Plany DRP	
Bezpieczeństwo osobowe	Polityka kadrowa. Polityka udzielania dostępów i uprawnień	Kompetencje dostosowane do realizowanych procesów.	Monitorowanie działań osób z wewnątrz organizacji „insider threats”	Eliminacja zachowań niepożądanych	Działania korygujące	

	Zarządzanie ryzykiem	Bariera	Zarządzanie ciągłością			Ewaluacja
	Zapobieganie		Przygotowanie	Reagowanie	Odtwarzanie	
Bezpieczeństwo tele-informatyczne IT/OT	Separacja sieci. Strefy zdemilitaryzowane. System zarządzania dostępami. Kryptografia Ochrona przed szkodliwym oprogramowaniem	IDS, intrusion detection system SIEM Security Information and Event Management	Kopie zapasowe	Zespół reagowania na incydenty komputerowe+ procedury	Sprzęt procedury odtwarzania z kopii zapasowych	

	Zarządzanie ryzykiem	Bariera	Zarządzanie ciągłością			Ewaluacja
	Zapobieganie		Przygotowanie	Reagowanie	Odtwarzanie	
Bezpieczeństwo fizyczne	Plan ochrony	zabezpieczenia	Plan działań na wypadek przełamania ochrony	Zespół interwencyjny	Analiza incydentów	
Bezpieczeństwo techniczne	Plany modernizacji i inwestycji oraz wdrażania nowych technologii	Rutynowe przeglądy, konserwacje i serwisowanie	Plan działań przeciwawaryjnych	Procedury reakcji na awarię	Procedury odtwarzania zużytych zasobów, aktualizacja zasad przeciwawaryjnych	

	Zarządzanie ryzykiem	Bariera	Zarządzanie ciągłością			Ewaluacja
	Zapobieganie		Przygotowanie	Reagowanie	Odtwarzanie	
Bezpieczeństwo prawne /polityka zgodności z prawem/	Własność zasobów; Przestrzeganie prawa własności Działania antykorupcyjne.	Umowy zabezpie-czające interes organizacji	Komunikowanie	Zespół prawny	Działania korygujące	

Ewaluacja

Art. 5h. 1**. Operator infrastruktury krytycznej** sporządza do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

2. Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące ochrony infrastruktury krytycznej w zakresie:

1) zapewnienia bezpieczeństwa fizycznego;
2) zapewnienia bezpieczeństwa technicznego;
3) zapewnienia bezpieczeństwa osobowego;
4) zapewnienia bezpieczeństwa teleinformatycznego;
5) zapewnienia bezpieczeństwa prawnego;
6) planów ciągłości działania i odtwarzania.

3. Raport o stanie ochrony infrastruktury krytycznej sporządza się z uwzględnieniem:

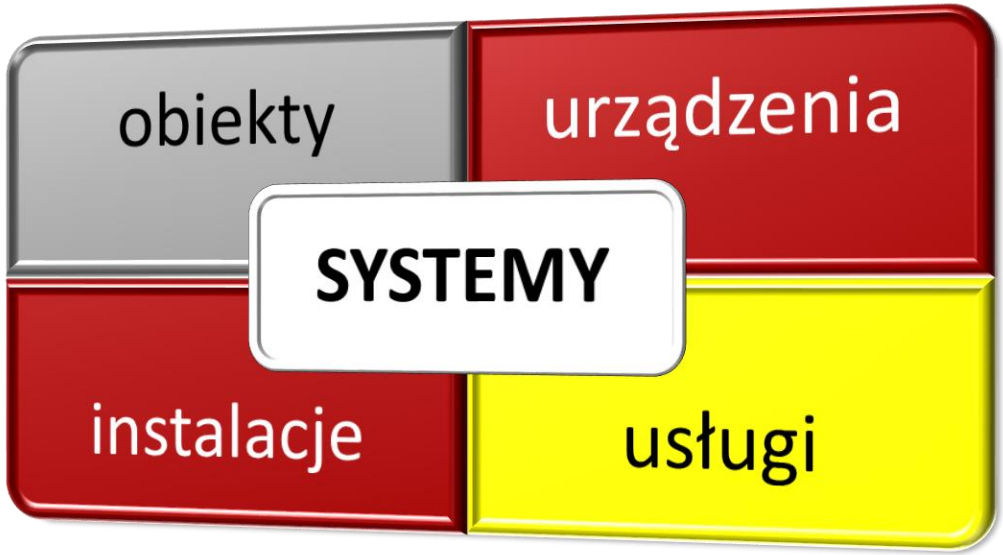
1) rozwiązań zawartych w planie ochrony infrastruktury krytycznej operatora;
2) wystąpienia ryzyka dla infrastruktury krytycznej zidentyfikowanego w planie ochrony infrastruktury krytycznej;
3) incydentów i zdarzeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, a nie były uwzględnione w planie ochrony infrastruktury krytycznej;
4) **wyników przeprowadzonych kontroli i audytów odnoszących się do zabezpieczeń zawartych w planie ochrony infrastruktury krytycznej;**
5) **opisu działań podjętych przez operatora w przypadkach, o których mowa w pkt 2 4.**

Zintegrowane zarządzanie bezpieczeństwem

- Fizyczna
- Techniczna
- Osobowa
- Teleinformatyczna (IT i OT)
- Prawna
- ~~Plany odbudowy~~ Plan ciągłości działania i odtwarzania

Spodziewane efekty wdrożenia postanowień NPOK 2021

1. Zidentyfikowane usługi kluczowe z punktu widzenia państwa oraz społeczności lokalnych.
2. Zidentyfikowane usługi kluczowe dla operatorów IK (współzależności usług).
3. Wyodrębnione sub-usługi i procesy składające się na usługę kluczową w ramach właściwego systemu (sektora) IK.
4. Opracowano wykaz obiektów IK biorąc pod uwagę ich możliwy wpływ na usługę kluczową (jej przerwanie , ograniczenie lub falsyfikację polegającą na odstępstwie od wymaganej jakości).



- **kluczowe dla bezpieczeństwa państwa i jego obywateli**
- **służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców**

RCB

?

witold.skomra@rcb.gov.pl