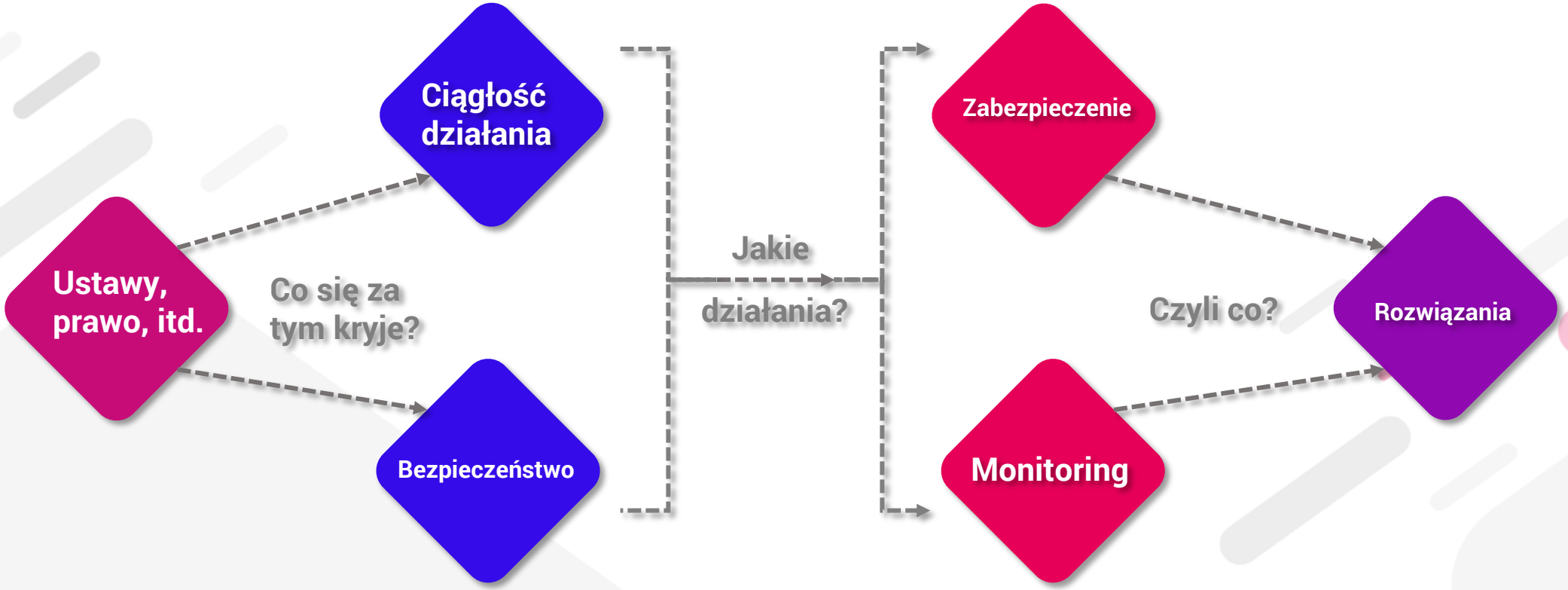
Podejścia do wdrożenia ustawy o krajowym systemie cyberbezpieczeństwa

Bartłomiej Chojnowski
Inżynier ds. Bezpieczeństwa IT
w firmie Passus SA

Ustawa o krajowym systemie cyberbezpieczeństwa

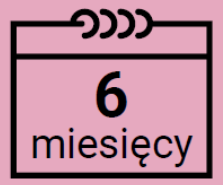
- wejście w życie: 28.08.2018 r.
- obowiązywanie: podmioty realizujące usługi kluczowe i usługi cyfrowe



Operatorzy kluczowi

Lp.	Kategorie OUK	Ilość podmiotów
1.	Energia	98
2.	Transport	83
3.	Bankowość i infrastruktura rynków finansowych	67
4.	Ochrona zdrowia	244
5.	Zaopatrzenie w wodę pitną i jej dystrybucja	31
6.	Usługi DNS/Punkty wymiany ruchu interne-towego (IXP)/prowadzenie rejestru domeny najwyższego poziomu TLD	8
		531 podmiotów

Zadania dla operatorów usług kluczowych

Zadania jakie ustawodawca nakłada na operatorów usług kluczowych z terminami na ich wykonanie (czas liczony od daty decyzji administracyjnej).	
	Analiza ryzyka, wyznaczenie osoby kontaktowej, zarządzanie incydentami, usunięcie podatności oraz prowadzenie działań w zakresie budowania świadomości
	Wdrożenie środków technicznych i organizacyjnych, zebranie informacji o podatnościach i incydentach, wdrożenie w życie wypracowanej dokumentacji, wdrożenie mechanizmów minimalizujących prawdopodobieństwo i skutki incydentów
	Przeprowadzanie audytu w myśl ustawy i przekazywanie sprawozdań z audytu wskazanym w ustawie podmiotom

Czym (nie) jest cyberbezpieczeństwo?

- nie jest tylko wdrożeniem systemu SIEM
- nie jest tylko ustanowieniem SOC/CSIRT
- nie jest tylko wdrażaniem zaawansowanych narzędzi monitorowania bezpieczeństwa
- nie jest tylko ustaleniem wektorów ataków i procedur reakcji
- nie jest tylko żadnym pojedynczym działaniem, o których dotychczas mowa była w literaturze dotyczącej wdrożenia dyrektywy NIS

Elementy składowe wdrożenia wymagań UKSC

Audyt pod kątem spełnienia wymagań ustawy ma dać przede wszystkim odpowiedź na pytanie, na jakim poziomie dojrzałości w zakresie cyberbezpieczeństwa jest moja organizacja.

Strategia bezpieczeństwa usług kluczowych/cyfrowych jest planem dojścia do docelowej dojrzałości bezpieczeństwa organizacji.

Mechanizm zarządzania ryzykiem jest dzisiaj podstawą do rozwiązywania problemów na wielu płaszczyznach. Systematyczne szacowanie ryzyka i zarządzanie nim powinno być podłożem systemu zarządzania bezpieczeństwem.

Zarządzanie incydentem to skuteczna identyfikacja, reakcja na incydent oraz raportowanie i wyciąganie wniosków. Stanowi ono obowiązek każdego operatora usługi kluczowej i usługi cyfrowej.

Systematyczna weryfikacja bezpieczeństwa systemów pozwala uzyskać informacje, gdzie tkwi ewentualna słabość, która może być wykorzystana przez atakującego

Zarządzanie systemami IT już od dawna nie polega wyłącznie na administrowaniu nimi. Aby mieć pełną kontrolę nad systemem, musimy nadzorować wszelkie zmiany wprowadzane przez podwykonawców i własnych pracowników.

„Cudowne” narzędzia, ludzie

- najdoskonalsze narzędzia
- najdoskonalsze cyberprocedury
- automatyzacja procesu zarządzania cyberbezpieczeństwem

- procedury > rozwiązania > zespół
- zespół > ludzie > rozwój

Cele bezpieczeństwa a normy

- Przykład wytycznych ENISA: „Technical Guidelines for the implementation of minimum security measures for Digital Service Providers” – 17.02.2017r.
- Przyjęcie jednego z 3 standardów bezpieczeństwa (podstawowy, sektorowy oraz najwyższy).
- 27 celów bezpieczeństwa do spełnienia. Każdemu celowi służą poszczególne środki bezpieczeństwa.
- Wytyczne wyjaśniają, w jaki sposób poszczególne kluczowe obszary bezpieczeństwa mogą być realizowane w oparciu o uznane, międzynarodowe normy

Cele bezpieczeństwa a normy

OBSZAR BEZPIECZEŃSTWA

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES[17]
SO1 Information Security Policy	●	●	●		●	●	●	●	
SO2 Risk management	●	●	●		●	●	●	●	
SO3 Security roles	●	●	●		●	●	●	●	
SO 04 Security in supplier relationships	●	●	●		●	●	●	●	
SO 05 Background checks	●	●	●		●	●	●	●	
SO 06 Security knowledge and training	●	●	●	●	●	●	●	●	
SO 07 Personnel changes	●	●	●		●	●	●	●	
SO 08 Physical and environmental security	●	●	●		●	●	●	●	
SO 09 Security of supporting utilities	●		●		●	●			
SO 10 Access control to network and information systems	●	●	●	●	●	●	●	●	●

NORMA REGULUJĄCA DANE ZAGADNIENIE

Cele bezpieczeństwa a normy

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES[17]
SO1 Information Security Policy	●	●	●		●	●	●	●	
SO2 Risk management	●	●	●		●	●	●	●	
SO3 Security roles	●	●	●		●	●	●	●	
SO 04 Security in supplier relationships	●	●	●		●	●	●	●	
SO 05 Background checks	●	●	●		●	●	●	●	
SO 06 Security knowledge and training	●	●	●	●	●	●	●	●	
SO 07 Personnel changes	●	●	●		●	●	●	●	
SO 08 Physical and environmental security	●	●	●		●	●	●	●	
SO 09 Security of supporting utilities	●		●		●	●			
SO 10 Access control to network and information systems	●	●	●	●	●	●	●	●	●
SO 11 Integrity of network and information systems	●		●		●	●	●	●	●
SO 12 Operating procedures	●				●	●			●
SO 13 Change management	●	●	●	●	●	●	●	●	●
SO 14 Asset management	●	●	●	●	●	●	●	●	●
SO 15 Security incident detection & response	●	●	●	●	●	●	●	●	
SO 16 Security incident reporting	●	●	●	●	●	●	●	●	
SO 17 Business continuity	●	●	●		●	●	●	●	

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES[17]
SO 18 Disaster recovery capabilities	●	●	●	●	●	●	●	●	
SO 19 Monitoring and logging policies	●	●	●		●	●	●	●	●
SO 20 System tests	●		●		●	●	●	●	●
SO 21 Security assessments	●	●	●		●	●		●	●
SO 22 Compliance	●	●	●		●	●			
SO 23 Security of data at rest	●	●	●	●	●	●	●	●	●
SO 24 Interface security		●	●		●	●		●	●
SO 25 - Software security		●	●		●	●	●	●	
SO 26 Interoperability and portability		●	●		●	●			
SO 27 Customer monitoring and log access	●	●	●	●	●	●	●	●	●

Dziękuję