DZP

więcej niż prawo

Cybersecurity – rosnące ryzyko prawne i reputacyjne

Bezpieczeństwo IT - Bezpieczeństwo prawne – Bezpieczeństwo Biznesu

Domański Zakrzewski Palinka sp. k.

Marzec 2016

Czy sami dbamy o nasze bezpieczeństwo?

Cyberprzestępczość w Polsce i na świecie

Cyberprzestępczość – globalne i lokalne trendy

Cyberprzestępczość jest na 2-gim miejscu wśród najczęściej raportowanych rodzajów przestępczości gospodarczej i dotyka już 32% organizacji.

Większość organizacji nie jest przygotowana i nie rozumie ryzyk związanych z tym rodzajem przestępczości - tylko 37% organizacji posiada procedurę działania na wypadek cyberataku.

Dane za: PwC Global Economic Crime Survey 2016

Zaledwie 45 proc. firm na świecie ma zaufanie do swych obecnych systemów cyberzabezpieczeń.

Cisco 2016 Annual Security Report

Cyberprzestępczość – globalne i lokalne trendy

„90 proc. firm na świecie uważa, że jest niewystarczająco przygotowana na cyber ataki.”

Raport „The Global Risks 2015 „ - World Economic Forum (WEF)

Liczba wykrytych incydentów naruszających bezpieczeństwo informacji wzrosła w przeciągu roku o 46 proc. Dynamika wzrostu odnotowanych cyberataków na świecie wyniosła 38 proc.

Ponad połowa przedsiębiorstw w Polsce odnotowuje co najmniej sześć cyberataków w przeciągu roku.

Najczęściej prowadziły one do utraty klientów i strat finansowych (po 33 proc. wskazań), ujawnienia lub zmiany danych wrażliwych (31 proc.) i utraty reputacji (16 proc.).

PWC, Badanie Stanu Bezpieczeństwa Informacji w Polsce 2016

DZP

Cyberprzestępczość to nie tylko problem globalny

Z polskiej kancelarii prawnej wykradziono dane, haker domaga się okupu za ich niepublikowanie

Uwaga! Oszuści atakują klientów tego banku!

"Potężny atak" na MON. Z serwerów ministerstwa skradziono tysiące e-maili

2015-12-01 07:34

Awaria systemów PLL LOT po ataku hakerskim już opanowana

Najbardziej rozpowszechnione cyberzagrożenia

Ataki organizowane przez państwa	• pozyskiwanie informacji • penetracja i obserwowanie systemów • działalność długofalowa
Działania aktywistów, hakerów, działania jednostek	• celem uzyskanie rozgłosu lub wywarcie nacisku • akcje jednorazowe
Zorganizowana cyberprzestępczość	• kradzież pieniędzy, tajemnic handlowych, danych osobowych • celem jest uzyskanie szybkich korzyści
Pracownicy obecni i byli	• działania dla własnej korzyści • zemsta • niefrasobliwość

Nowe regulacje prawne - nowe ryzyka?

Ustawa o Policji

- Obowiązek zapewnienia warunków technicznych i organizacyjnych dla działalności operacyjnej służb mundurowych;
- Możliwość pozyskiwania przez służby danych o lokalizacji urządzeń mobilnych oraz odbiorcach i nadawcach wiadomości bez wiedzy użytkowników

Rozporządzenie o ochronie danych osobowych

- Zaostrzone wymogi w zakresie ochrony danych osobowych
- Regularne audyty i kontrole
- Kary za naruszenie obowiązków aż do kwoty do 20 mln euro lub 4% rocznego, światowego obrotu (co jest większe)

Dyrektywa o cyberbezpieczeństwie

- **Nowe, szerokie obowiązki informacyjne**
  - Operatorzy infrastruktury krytycznej w sektorach finansowym, transporcie, energetyce i ochronie zdrowia.
  - Firmy IT, sklepy internetowe, platformy płatnicze, wyszukiwarki, media społecznościowe.
  - Administracja publiczna.

Co robić?

V.

Co robić?

- Kultura bezpieczeństwa
- Właściwa struktura organizacyjna
- Właściwe procedury i regulacje wewnętrzne
- Infrastruktura techniczna IT

KONIECZNE JEST KOMPLEKSOWE PODEJŚCIE

KTO NIE KONTROLUJE TEN NIE MA KONTROLI

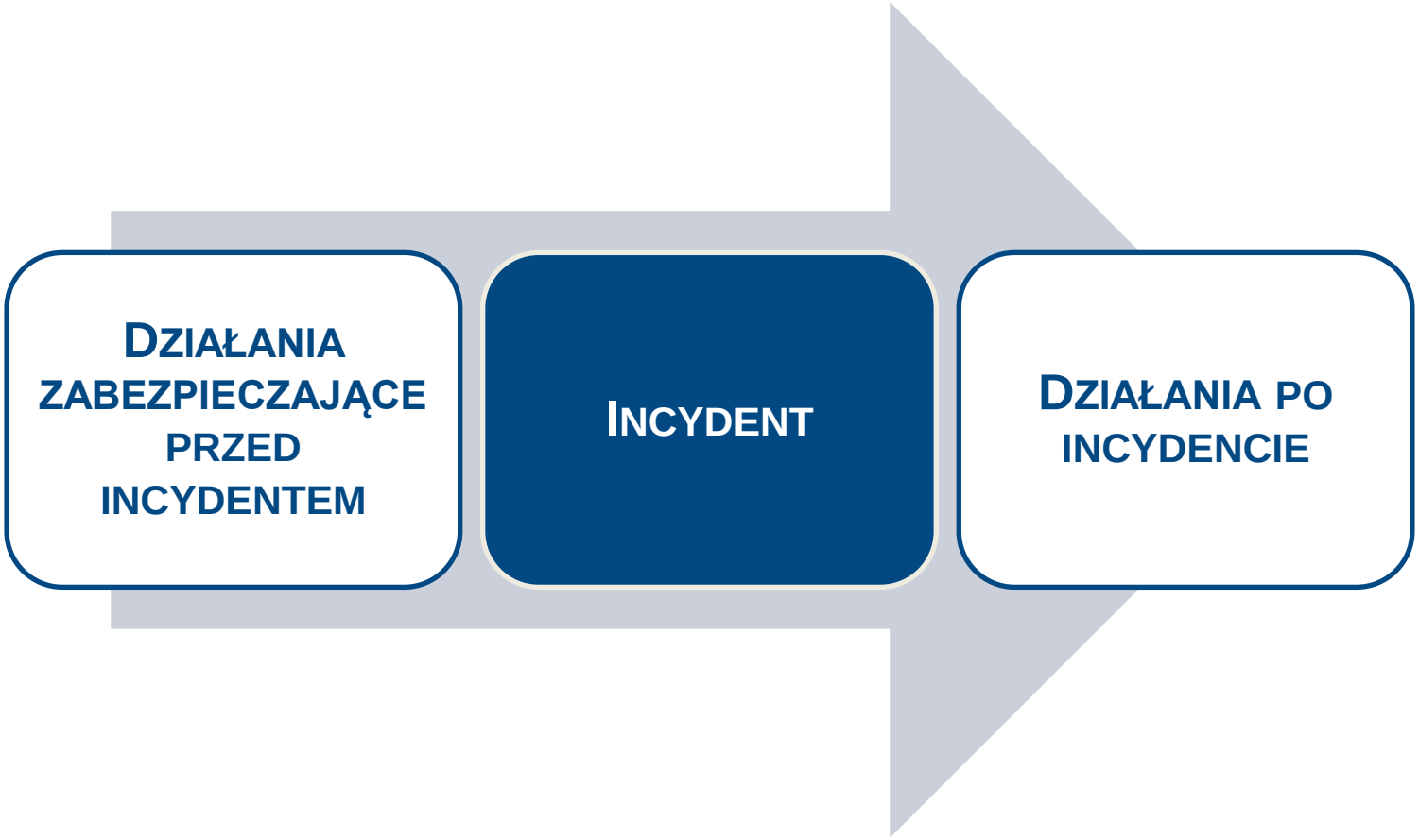
- Konieczność regularnych audytów
- Regularne testy i ćwiczenia

Jakie informacje należy chronić?

- Tajemnica bankowa, ubezpieczeniowa i „maklerska”
- Tajemnica lekarska
- Dane osobowe, w szczególności dane wrażliwe
- Tajemnice handlowe
- Własność intelektualna
- Dane klientów

Podejście holistyczne

Każdy etap procesu



Działania zabezpieczające przed incydentem

- Audyt prawny
- Opracowanie i wdrożenie polityk wewnętrznych
- Szkolenia dla managerów i pracowników
- Opracowanie i wdrożenie procedury kryzysowej
- Bieżące doradztwo dla Biura Zarządu, Działów IT, Compliance, Prawnego oraz PR.

Etap I: Audyt prawny – bezpieczeństwo IT

Analiza umów zawartych z dostawcami rozwiązań IT	analizy umów z partnerami handlowymi firmy pod kątem bezpieczeństwa	Weryfikacja istniejących procedur bezpieczeństwa, w tym działań związanych z postępowaniem po incydencie
Audyt procedur i dokumentacji wewnętrznej dot. obowiązków pracowników w zakresie bezpieczeństwa IT	Analiza polityk bezpieczeństwa, regulaminów	Analiza stosowanych wzorców umów o pracę, współpracę, zlecenia, o dzieło,
Analiza dokumentacji pracowniczej pod względem bezpieczeństwa informacji i systemów IT	Weryfikacja wyznaczenia odpowiednich osób odpowiedzialnych za bezpieczeństwo IT	Standaryzacja umów IT oraz wdrożenie procedury weryfikacji dostawców rozwiązań IT

Etap II: Audyt prawny – dane osobowe

Analiza dokumentacji związanej z przetwarzaniem danych osobowych ze szczególnym uwzględnieniem wymogów Cloud Computing

Ocena struktury wewnętrznej przedsiębiorstwa pod kątem wymogów bezpieczeństwa przetwarzania danych osobowych

Analiza bezpieczeństwa przetwarzanych danych pod kątem zakresu uprawnień użytkowników

Ocena spełnienia wymogów prawych dotyczących technicznych aspektów danych np. takich jak format zapisu i możliwość eksportu

Audyt prawny – media społecznościowe

Analiza prawna dotycząca obecności firmy i jej kluczowego personelu w mediach społecznościowych .

Wskazanie ryzyk prawnych związanych z naruszeniami tajemnicy przedsiębiorstwa, danych osobowych, własności intelektualnej, „dziur” w systemie bezpieczeństwa itp.

Analiza umów o pracę, regulaminów, kodeksów postępowania. Propozycja rozwiązań.

Weryfikacja umów zawieranych z mediami społecznościowymi oraz partnerami obsługującymi aktywności.

Audyt prawny – polityka w zakresie *BYOD (Bring Your Own Device)*

Analiza Polityki i praktyki BYOD w Firmie

Ocena ryzyk prawnych

Propozycje regulacji pracowniczych

Audyt prawny – wymogi sektorów regulowanych

Analiza standardowych umów zawieranych z klientami z sektorów regulowanych;

Weryfikacja aktualnych rozwiązań pod kątem spełnienia prawnych oraz technicznych obowiązków ustawowych

Wymogi dotyczące outsourcingu w działalności bankowej, ubezpieczeniowej, działalności firm inwestycyjnych, instytucji płatniczych, funduszy inwestycyjnych i funduszy emerytalnych

Ochrona danych objętych tajemnicą profesjonalną w działalności regulowanej, np. w branży medycznej

Opracowanie i wdrożenie procedury kryzysowej

Opracowanie zasad postępowania w sytuacji incydentu

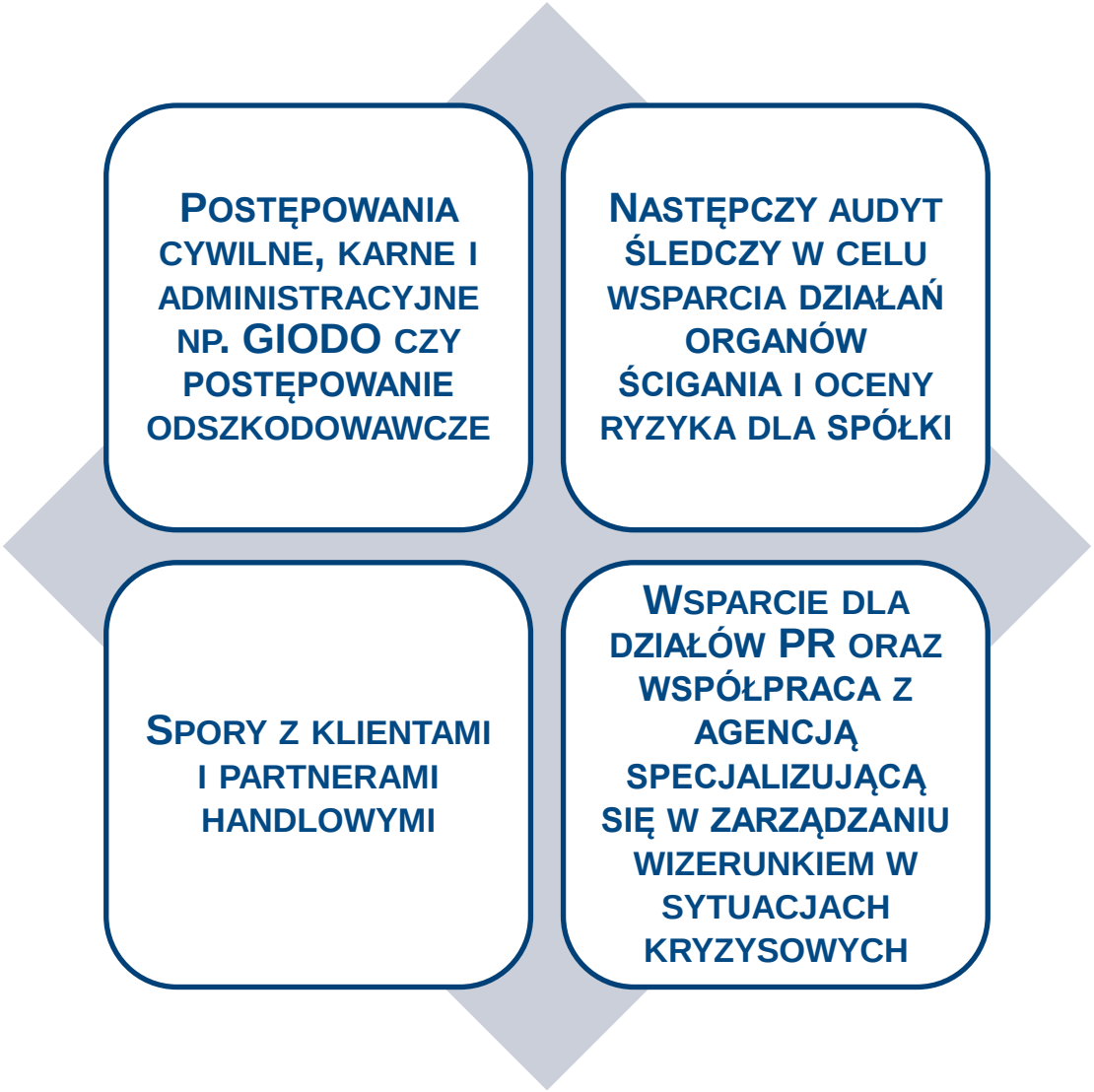
Określenie osób odpowiedzialnych za podejmowanie decyzji w sytuacji incydentu

Dopasowanie treści polityki do istniejącego już w ramach organizacji systemu compliance

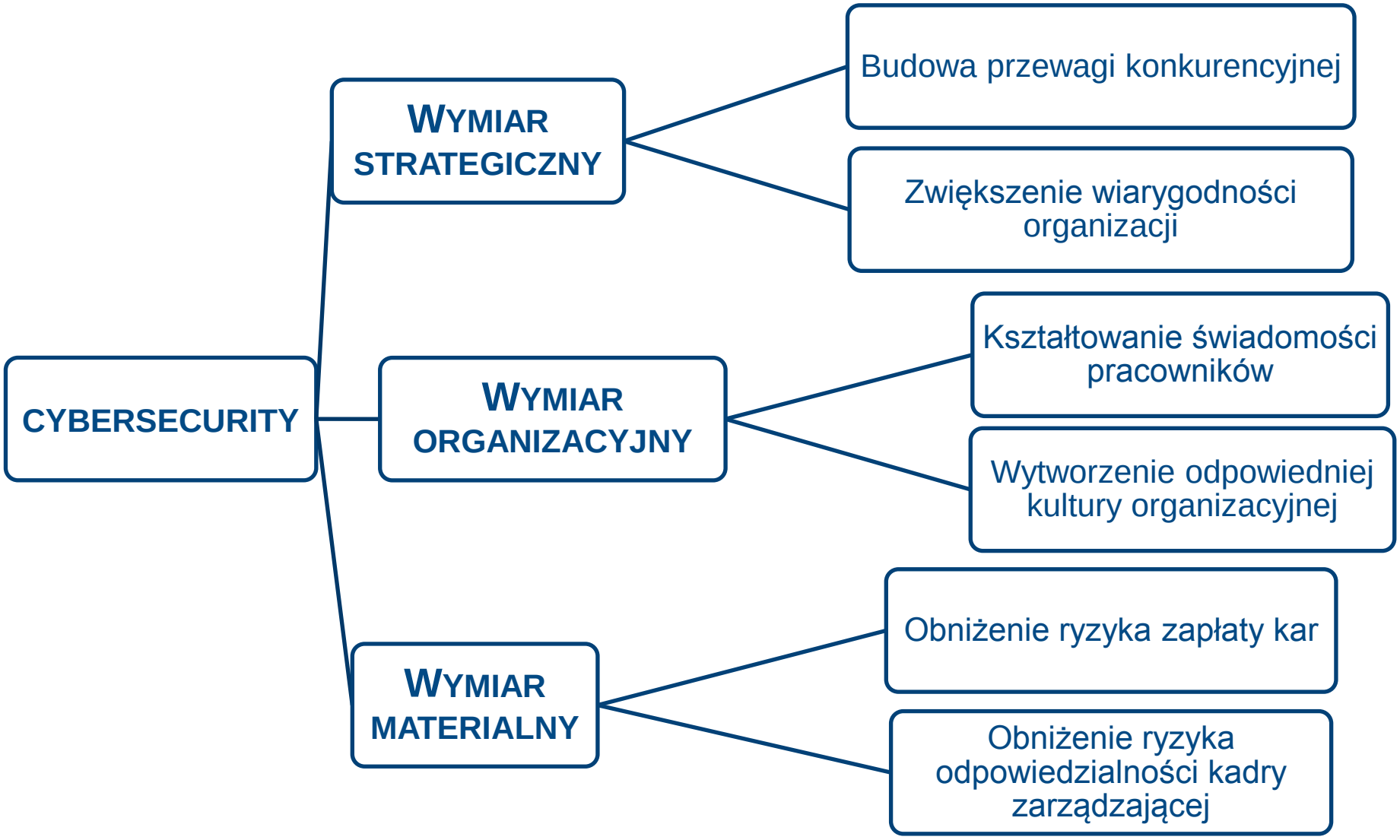
Wskazanie głównych punktów ryzyka w sytuacji kryzysowej

Działanie w czasie incydentu

Kompleksowe działania ochronne po incydencie



Efekty podejścia kompleksowego



Nasze doświadczenia

Narodowy przewoźnik lotniczy

- **Przygotowanie oceny prawnej charakteru i zakresu odpowiedzialności dostawców systemów bezpieczeństwa IT oraz urządzeń i usług sieciowych**
- **Opracowanie strategii postępowania w celu dochodzenia roszczeń odszkodowawczych** od dostawców systemów bezpieczeństwa IT
- **Zabezpieczenie materiału dowodowego**.
- **Kompleksowa obsługa sporu z dostawcami systemów bezpieczeństwa IT.**

Międzynarodowy koncern energetyczny

- **Opinia prawna dot. ewentualnej odpowiedzialności banku obsługującego Klienta.**
- **Przygotowanie strategii dotyczących roszczeń odszkodowawczych.**
- **Złożenie wniosku o ściganie do odpowiednich organów.**
- **Nadzór i udział w postępowaniu przygotowawczym.**

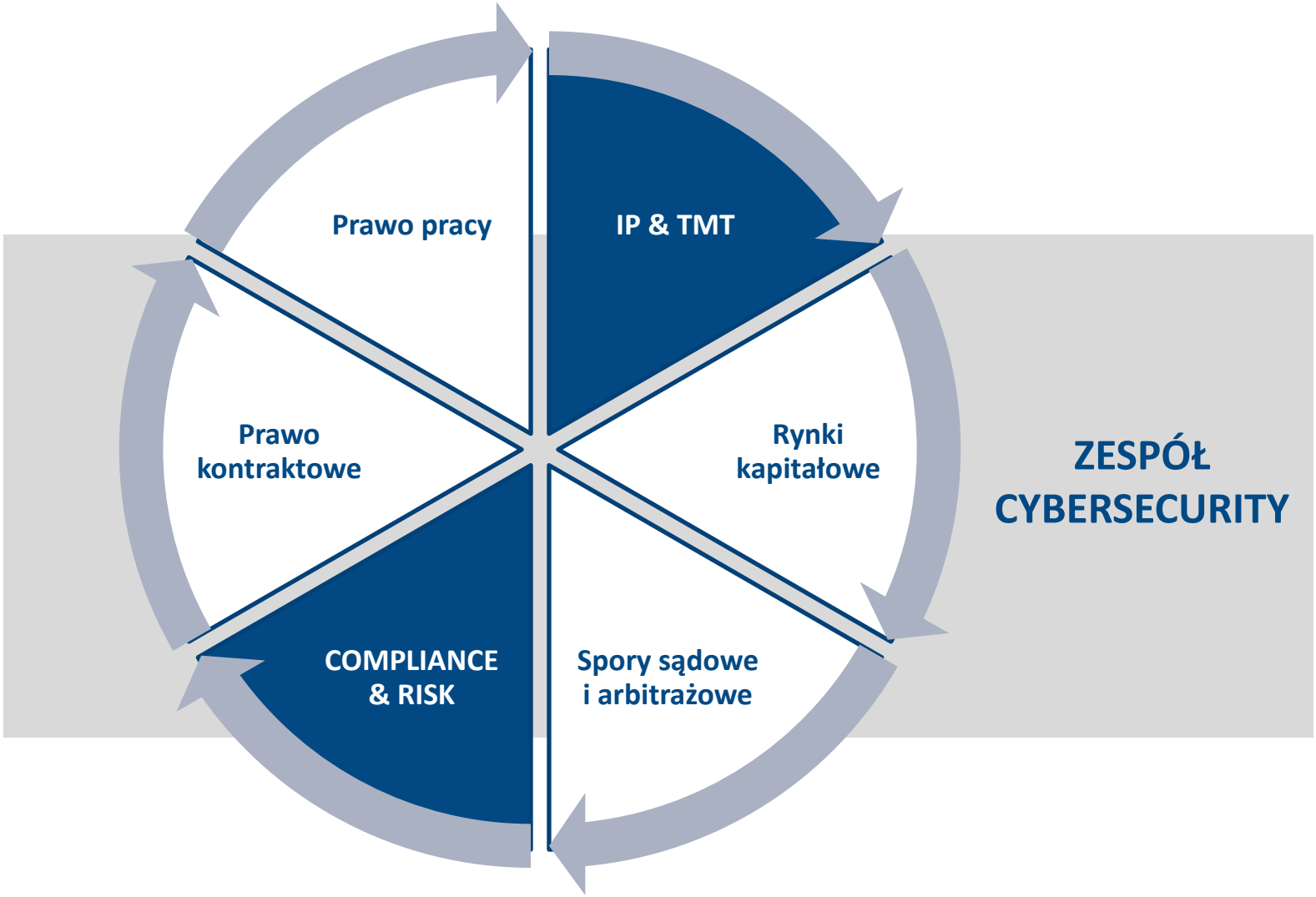
Wiodący komercyjny nadawca telewizyjny

- **Audyt umów z zakresu teleinformatyki**
- Analiza działalności telekomunikacyjnej
- Doradztwo strategiczne w zakresie zarządzenia zasobami teleinformatycznymi

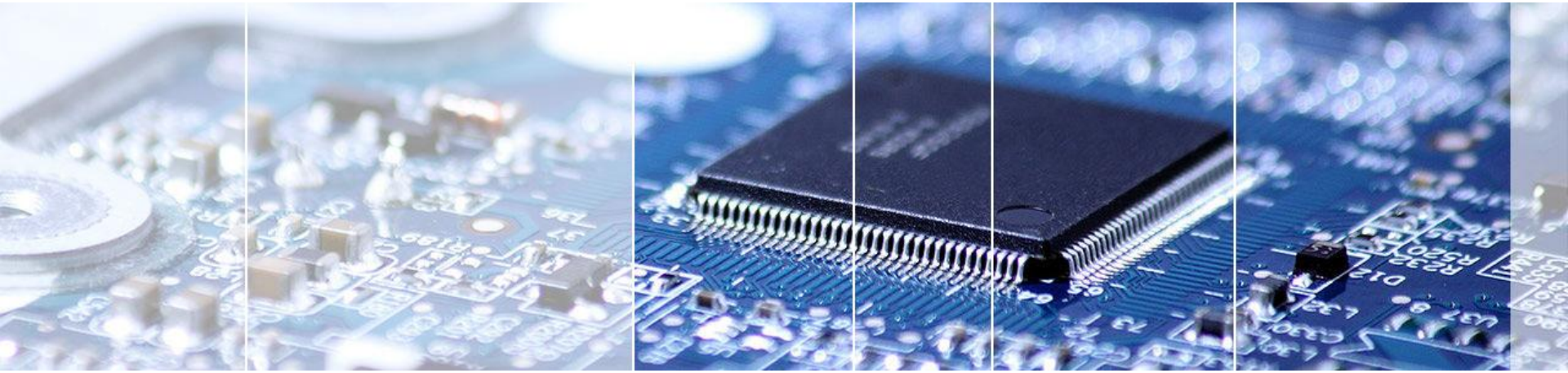
Zespół cybersecurity

DZP

Interdyscyplinarny zespół łączący specjalistów z kilku dziedzin prawa



DZP



Domański Zakrzewski Palinka sp. k.

Warszawa | **Rondo ONZ 1 | 00-124 Warszawa**
T: +48 22 557 76 00 | F: +48 22 557 76 01

Poznań | ul. Paderewskiego 8 | 61-770 Poznań
T: +48 61 642 49 00 | F: +48 61 642 49 50

Wrocław | ul. Gwiaździsta 66 | 53-413 Wrocław
T: +48 71 712 47 00 | F: +48 71 712 47 50

www.dzp.pl www.linkedin.com/company/dzp