Jak sobie POŚCIELESZ tak się WYŚPISZ – czyli o tym jak dobrze odrobić pracę domową w zakresie zarządzania incydentami.

Piotr Kawczyński – FORSAFE Sp. Z o.o.

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

02.02.2023r.

Zajmuję się szeroko pojętym bezpieczeństwem informacji od 2004 roku. Posiadam wieloletnie doświadczenie w obszarze bezpieczeństwa informacji poparte praktyką i kompetencjami m.in.: Audytora Wiodącego i Audytora Wewnętrznego (ISO 27001/27701/22301) a także licznych certyfikacji takich jak Certified Data Privacy Solutions Engineer (ISACA Pro Member), Microsoft Certified Professional, Microsoft Certified Technology Specialist i innych. Posiadam upoważnienie dostępu do informacji niejawnych z klauzulą „poufne". Pełnię funkcję Inspektora Ochrony Danych w średnich i dużych przedsiębiorstwach. Biorę udział w licznych wydarzeniach branżowych związanych z tematyką bezpieczeństwa informacji jako prelegent oraz trener szkoleń (m.in.: Akademia BECK, Centrum Promocji Informatyki).

W latach 2013 – 2016 byłem wykładowcą na Podyplomowym Studium Ochrony Danych Osobowych, organizowanym przez Wydział Prawa i Administracji Uniwersytetu Łódzkiego pod patronatem Generalnego Inspektora Ochrony Danych Osobowych oraz ABW. Ukończyłem Podyplomowe Studium Ochrony Danych Osobowych, organizowane przez Wydział Prawa i Administracji Uniwersytetu Łódzkiego oraz Podyplomowe Studia Cyberbezpieczeństwo prowadzone przez Akademię Marynarki Wojennej w Gdyni.

Jestem członkiem założycielem Związku Firm Ochrony Danych Osobowych, członkiem Stowarzyszenia Praktyków Ochrony Danych oraz członkiem grupy roboczej ds. ochrony danych osobowych w Ministerstwie Cyfryzacji.

INCYDENTY

Definicja

Zdarzenie związane z bezpieczeństwem informacji

określony stan systemu zarządzania bezpieczeństwem informacji, usługi lub sieci, wskazujący na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji

INCYDENTY

Definicja

Incydent związany z bezpieczeństwem informacji

pojedyncze zdarzenie lub serie niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji

INCYDENTY

Definicja

Naruszenie bezpieczeństwa informacji

każdy przypadek naruszenia poufności, dostępności i integralności informacji, jak również niespełnienie wymagań dotyczących bezpieczeństwa informacji.

INCYDENTY

Definicja jednolita (subiektywna)

Incydent bezpieczeństwa to zidentyfikowane zdarzenie wskazujące na możliwe naruszenie triady atrybutów informacji tj. poufność, integralność, dostępność (CIA), mogące powodować znaczne szkody w organizacji, zagrozić działalności biznesowej i ujawnić poufne dane.

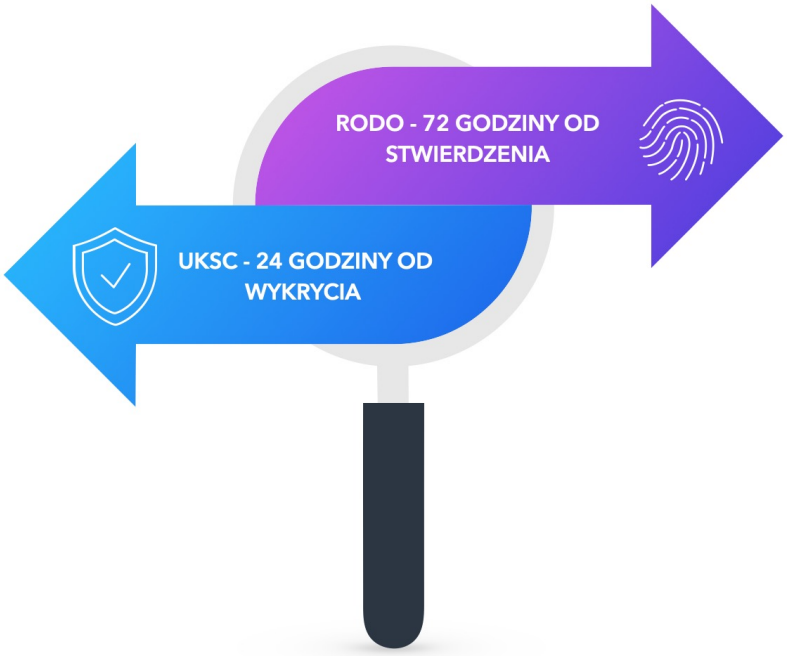
INCYDENTY

UKSC:RODO

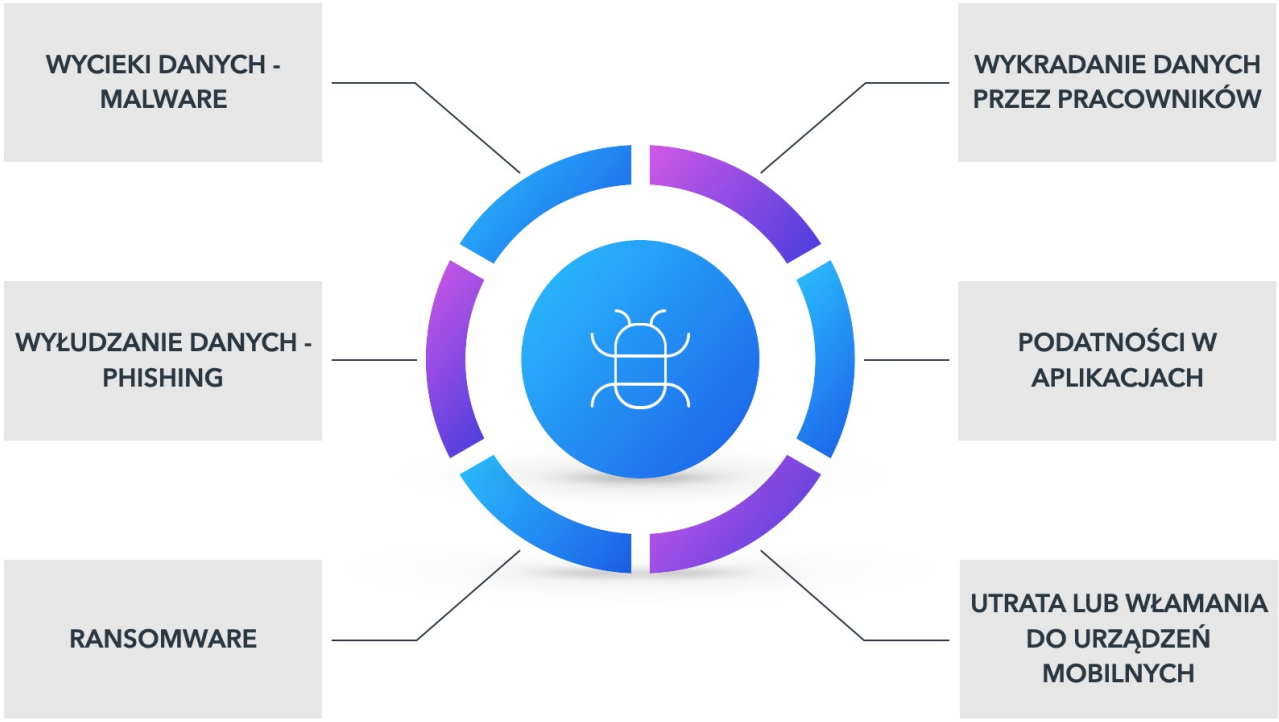
- art. 23 ust. 1 UKSC - obsługa incydentu: wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, działania naprawcze, ograniczanie skutków.

- art. 33 ust. 1 i 2 RODO - naruszenie ochrony danych skutkujące ryzykiem naruszenia praw i wolności osób fizycznych.

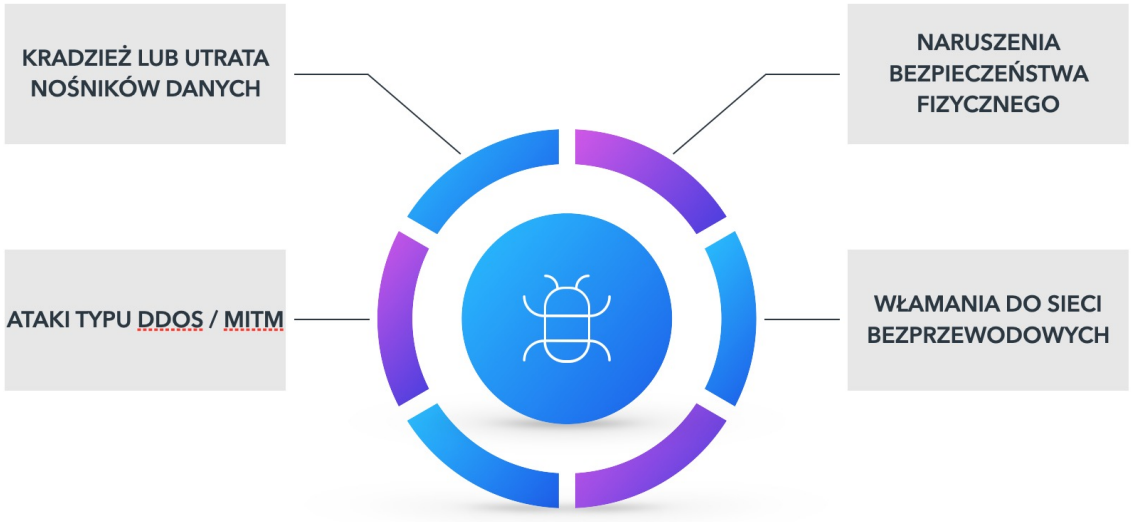
INCYDENTY - notyfikacja



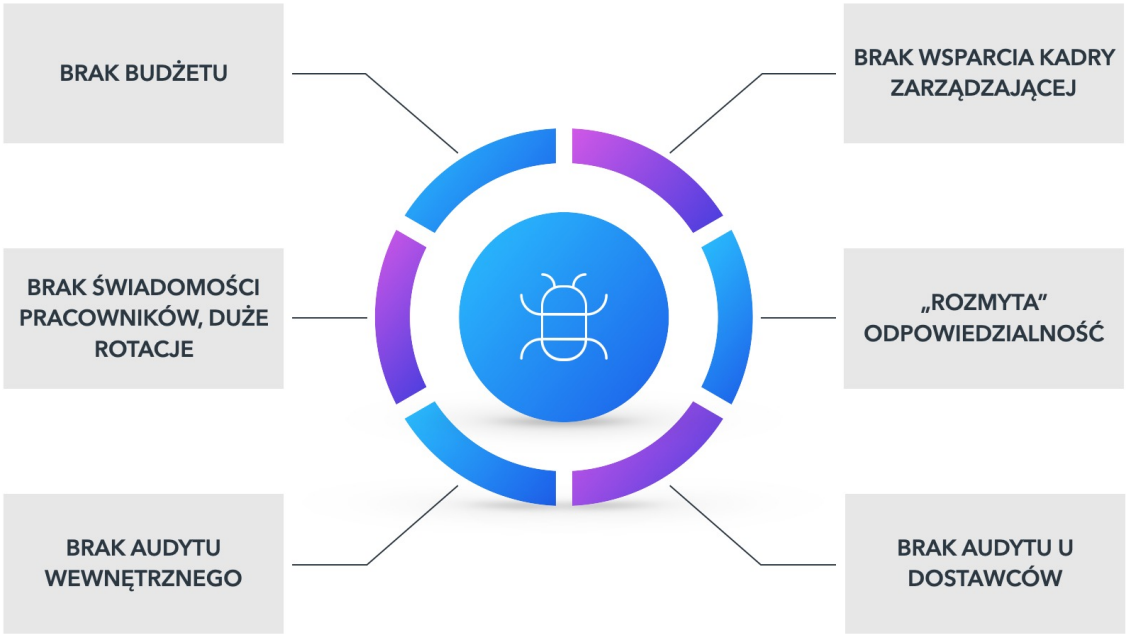
Źródła incydentów



Źródła incydentów



Źródła incydentów



Fazy zarządzania incydentami

wybór metodyki oceny naruszenia

określenie ról w zespole

wybór rozwiązania w którym naruszenie będzie obsługiwane

checklista

wzorce dokumentów

„druga para oczu”

rozliczalność

Korzyści z wdrożenia systemu zarządzania incydentami

1. Poprawienie ogólnego bezpieczeństwo informacji w organizacji.
2. Zmniejszenie negatywnego wpływu na biznes.
3. Zapobieganie incydentom związanym z bezpieczeństwem informacji.
4. Wnioski mogą uzasadniać budżet.
5. Zwiększenie efektywności oceny ryzyka bezpieczeństwa informacji.
6. Zwiększenie świadomości i kultury bezpieczeństwa.
7. Realne odzwierciedlenie w polityce bezpieczeństwa.


Dziękuję
za uwagę
PKAWCZYNSKI@FORSAFE.PL
WWW.LINKEDIN.COM/IN/PIOTRKAWCZYNSKI