PFR
Polski Fundusz Rozwoju

Sieć Firm Przyszłości

COMCERT

Jak uchronić organizację przed cyberatakami?

Podstawy Cyberbezpieczeństwa

Poznaj ofertę warsztatową PFR

20 lutego 2024, 10:00

Poznaj eksperta

Piotr Kępski

Obecnie pracuje jako Cybersecurity Systems Analyst w ComCERT S.A., gdzie zajmuje się obszarem modelowania zagrożeń w cyberprzestrzeni oraz TTP (techniki, taktyki i procedury) w cyberatakach. Audytor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO/IEC 27001. Posiada doświadczenie we wdrażaniu polityki ochrony informacji z wykorzystaniem ISO/IEC 27001 oraz w planowaniu i wdrażaniu polityk bezpieczeństwa infrastruktury i informacji cyfrowej na bazie ISO/IEC 27001, 27002, 27005. Przez wiele lat związany z obszarem utrzymania systemów IT w sektorze publicznym, zarówno na poziomie technicznym jak i zarządczym. Jako członek Fundacji Bezpieczna Cyberprzestrzeń aktywnie działa na rzecz wzmacniania świadomości w obszarze zagrożeń pochodzących z cyberprzestrzeni, w tym m. in. prowadzi szkolenia, współtworzy serię podcastów Cyber, Cyber… oraz bierze udział w organizacji rozgrywek Ligi CyberTwierdza.

Plan opowieści…

1. Dlaczego cyberbezpieczeństwo jest istotne?
   - Największe zagrożenia i incydenty w sektorze MŚP
   - Potencjalne konsekwencje
2. Od czego zacząć…
   - Inwentaryzacja zasobów
   - Identyfikacja zagrożeń
   - Plan działania
3. Jak się przygotować na cyberatak/incydent
   - Budżet
   - Kompetencje
   - Organizacja i procedury
   - Technologia
4. Incydent – mleko się rozlało, co dalej…

Dlaczego cyberbezpieczeństwo jest istotne?

- Wszechobecne systemy teleinformatyczne
- Ochrona danych osobowych
- Wymogi prawne
- Ochrona własności intelektualnej, tajemnicy handlowej i innych poufnych informacji
- Cyberzagrożenia są coraz bardziej zaawansowane

Dlaczego cyberbezpieczeństwo jest istotne?

Cyberatak - każdy rodzaj ofensywnego działania w Internecie osób lub organizacji, którego celem mogą być systemy informatyczne, sieci komputerowe, komputery lub inne urządzenia osobiste[1]

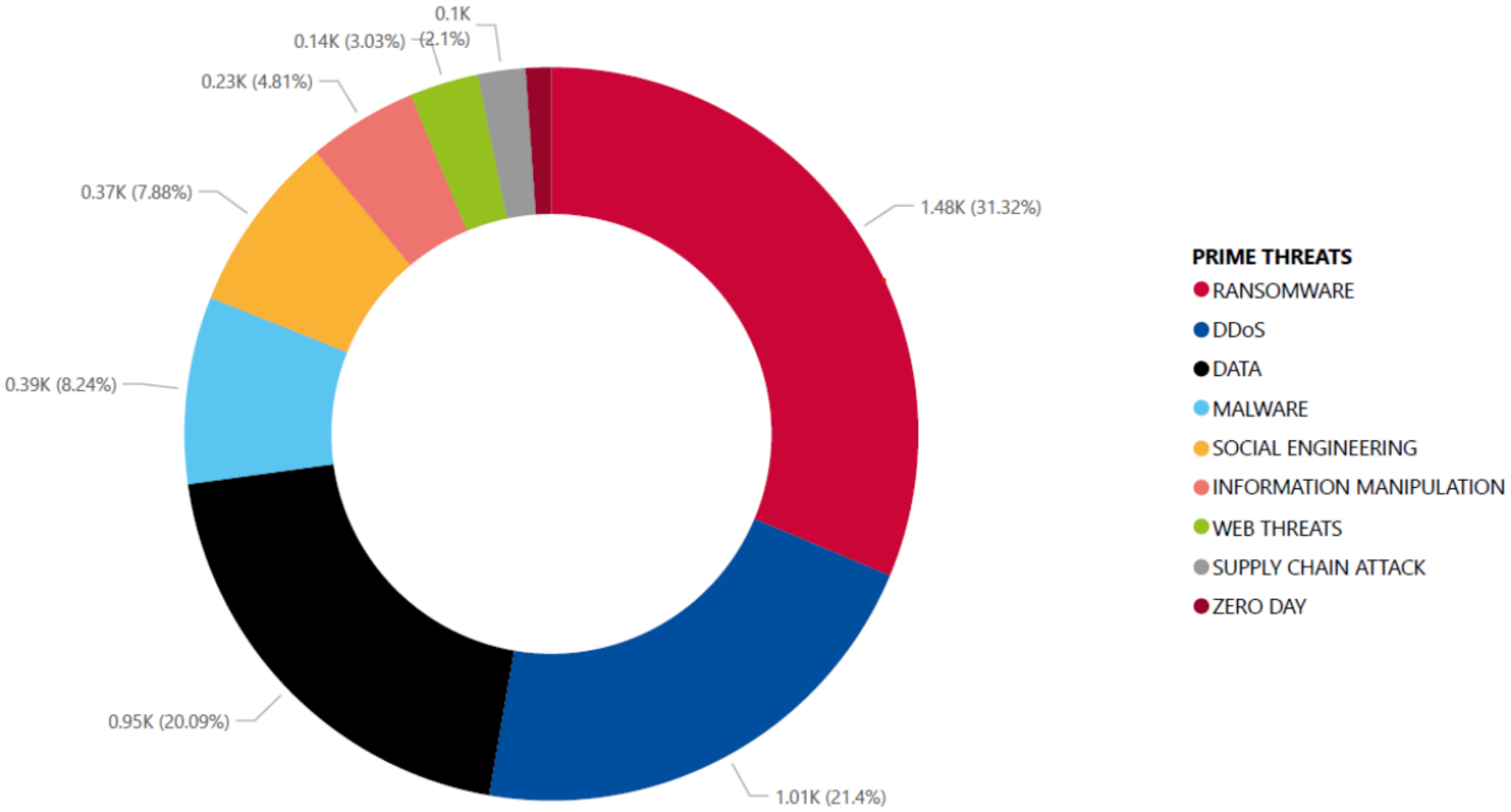
Najczęściej obserwowane cyberataki:

- Distributed Denial of Service (DDoS)
- Phishing
- Kradzież danych (wyłudzenie danych lub pieniędzy, itp.)
- Ransomware
- Inne…

[1] https://sjp.pwn.pl/sjp/cyberatak;5606168.html

Dlaczego cyberbezpieczeństwo jest istotne?

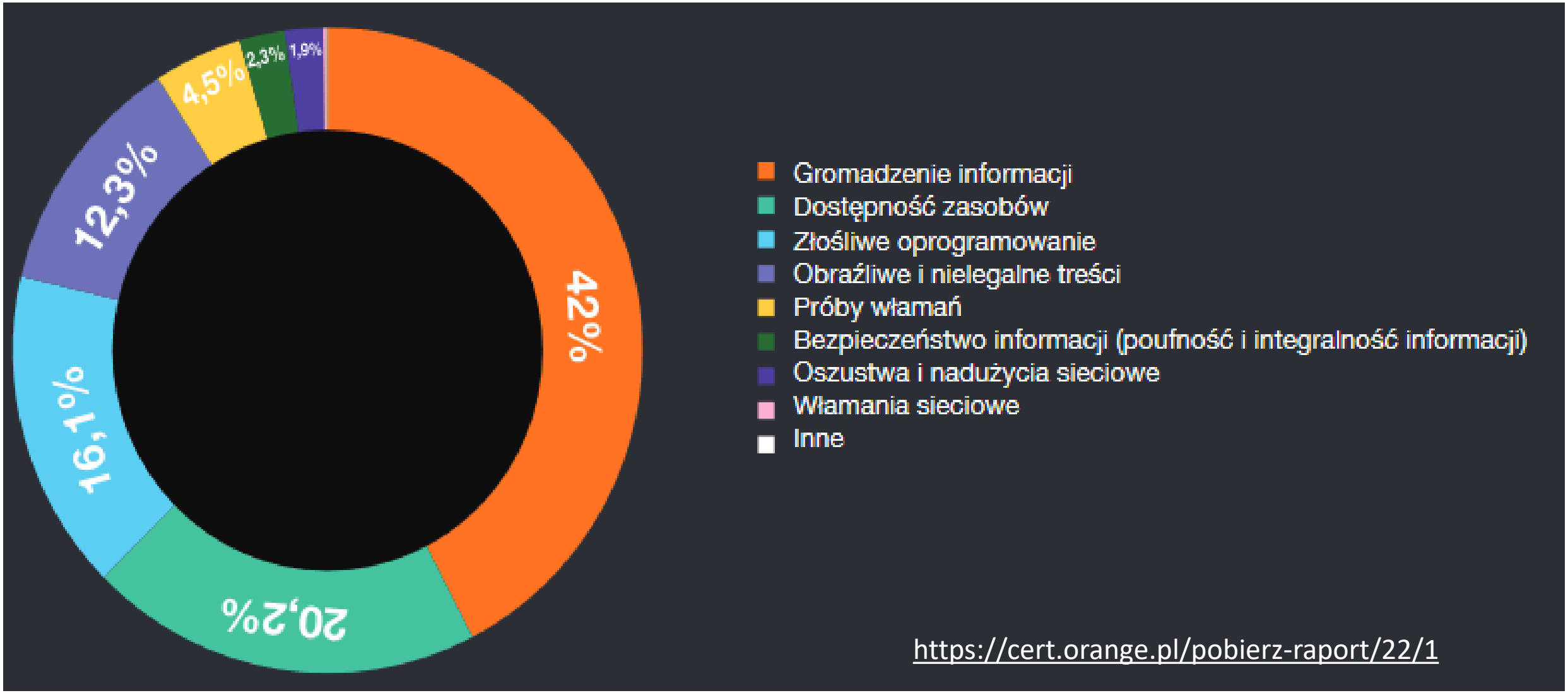
Najczęściej obserwowane cyberzagrożenia…



https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Dlaczego cyberbezpieczeństwo jest istotne?

Najczęściej obserwowane cyberzagrożenia…

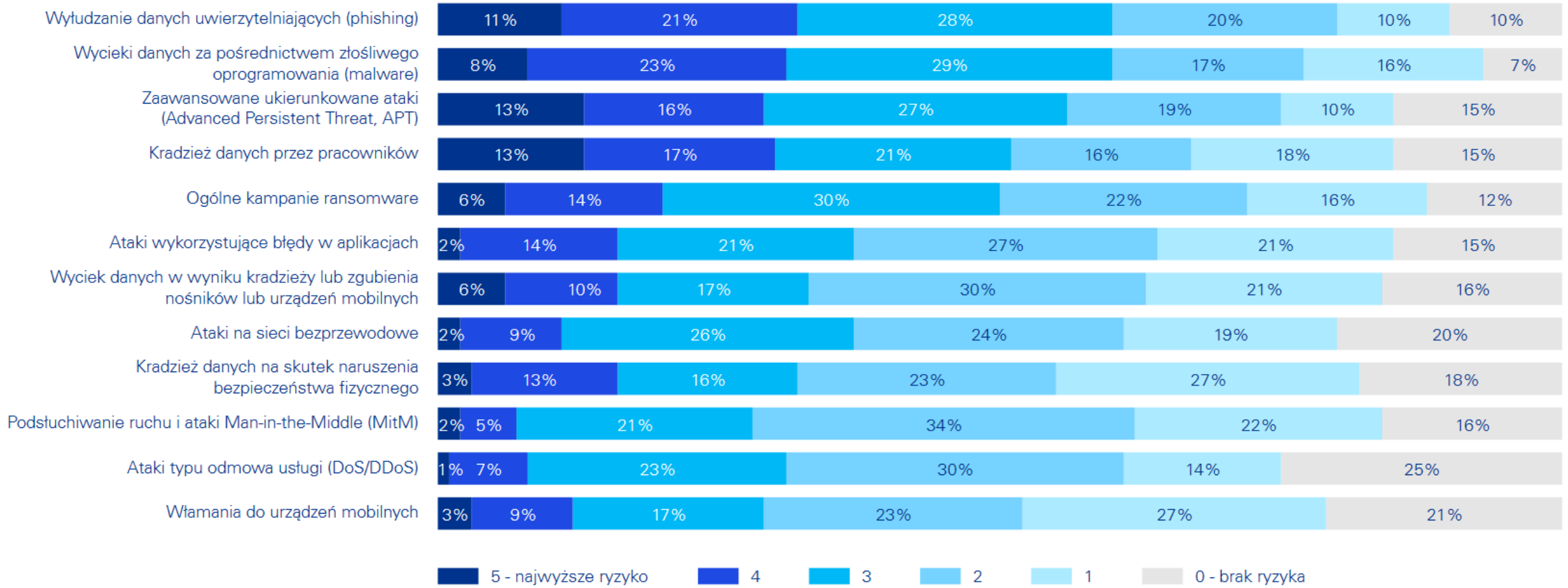


https://cert.orange.pl/pobierz-raport/22/1

Dlaczego cyberbezpieczeństwo jest istotne?

Najczęściej obserwowane cyberzagrożenia…

Które z poniższych cyberzagrożeń stanowią największe ryzyko dla organizacji?

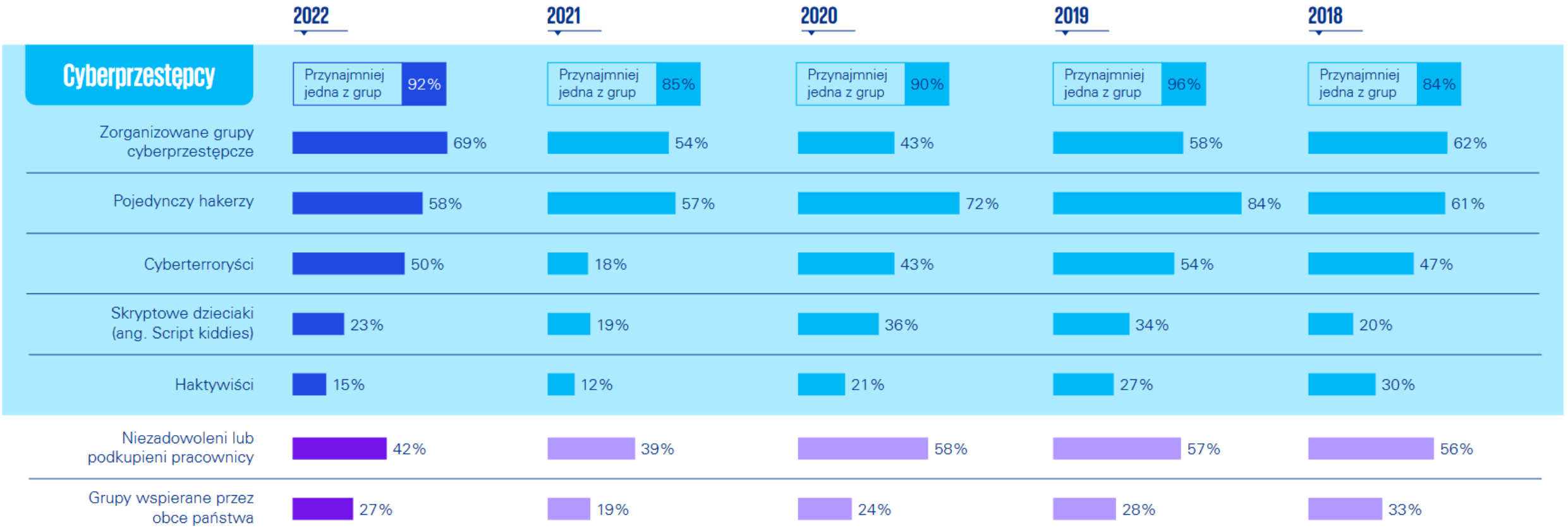


Barometr cyberbezpieczeństwa, KMPG

https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2022/05/pl-raport-kpmg-w-polsce-barometr-cyberbezpieczenstwa-ochrona-cyfrowej-tozsamosci-secured.pdf

Dlaczego cyberbezpieczeństwo jest istotne?

Kto nam zagraża?



Barometr cyberbezpieczeństwa, KMPG

https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2022/05/pl-raport-kpmg-w-polsce-barometr-cyberbezpieczenstwa-ochrona-cyfrowej-tozsamosci-secured.pdf

Dlaczego cyberbezpieczeństwo jest istotne?

Ataki APT (z ang. Advanced Persistent Threat) - złożone, długotrwałe i wielostopniowe działania kierowane przeciwko konkretnym osobom, organizacjom lub firmom (ataki ukierunkowane) wykorzystujące bardzo wyrafinowane metody i zaawansowane technologie do osiągnięcia zaplanowanego celu[1], który może być motywowany kwestiami politycznymi, ideologicznymi lub finansowymi

Atak APT jest zawsze starannie zaplanowany i zaprojektowany w celu infiltracji określonej organizacji oraz uniknięcia istniejących środków bezpieczeństwa.

Atak APT może być także rozłożony w dużym okresie czasu.

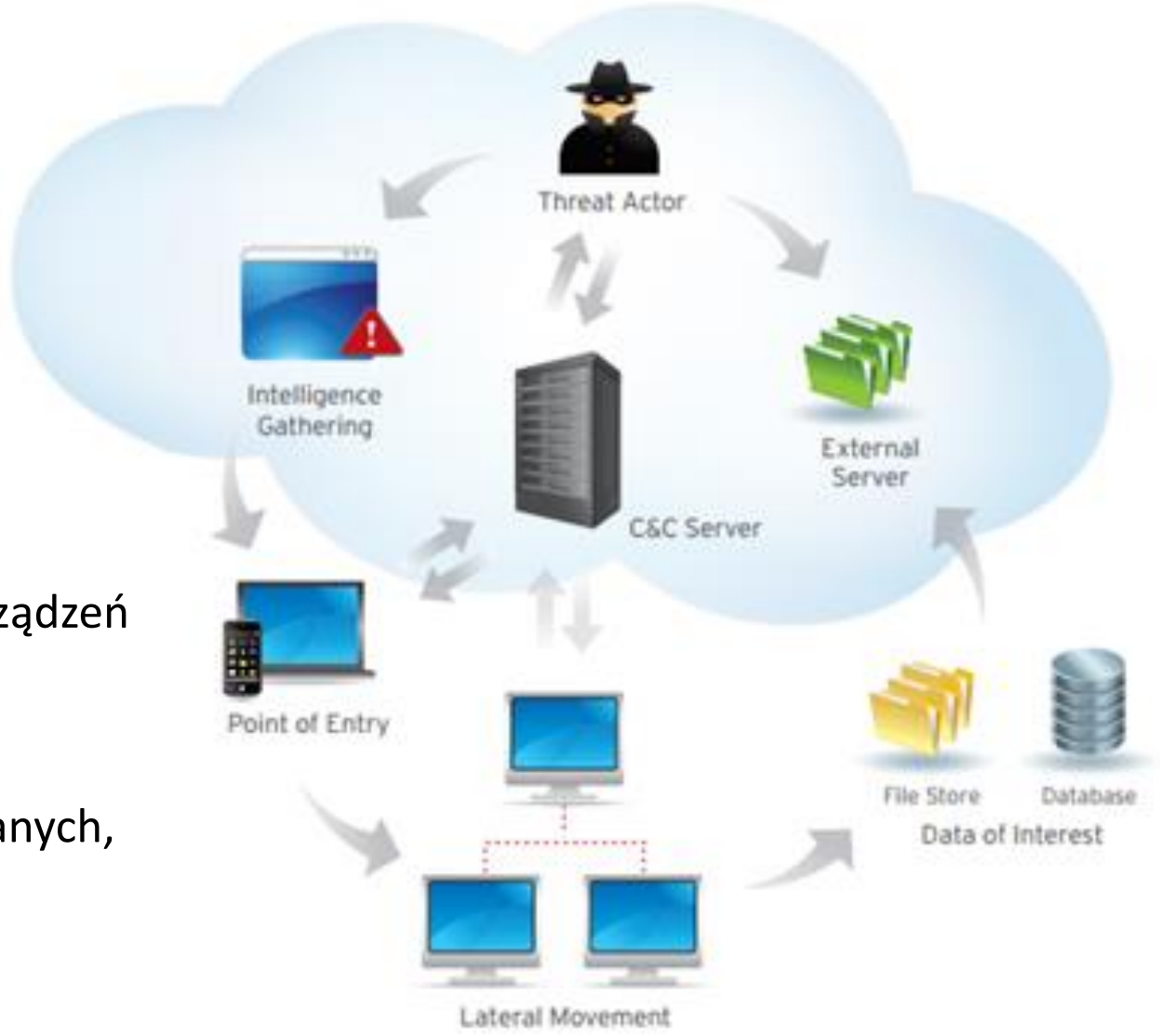
[1] https://www.cybsecurity.org/pl/ataki-apt-w-swietle-polskich-regulacji-prawnych/

https://en.wikipedia.org/wiki/Advanced_persistent_threat

Dlaczego cyberbezpieczeństwo jest istotne?

Anatomia (typowego) APT

1. Wybór celu
2. Przygotowania
3. Rekonesans
4. Początkowa kompromitacja
   - Wektor infekcji (np. spearphishing)
   - Instalacja malware, persystencja
5. Eskalacja uprawnień
6. Lateral movements - pozyskanie dostępu do innych urządzeń
7. Rekonesans środowiska
8. Realizacja celów ataku
   - Uzyskanie dostępu do kluczowych zasobów (bazy danych, serwery plików, kontroler domeny)
   - Eksfiltracja danych / destrukcja



Dlaczego cyberbezpieczeństwo jest istotne?

DDoS:

Skutki ataku DDoS				
utrata dostępu do danych i usług	zakłócenie ciągłości działania organizacji	konsekwencje prawne	konsekwencje finansowe	utrata reputacji

Metody infekcji				
e-mail zawierający złośliwy załącznik lub link	fałszywa strona WWW (kod złośliwy osadzony na stronie lub plik do pobrania)	nośnik pamięci (np. USB, płyta, itp.)	nielegalne (pirackie) oprogramowanie	Atak APT

Dlaczego cyberbezpieczeństwo jest istotne?

Kradzież danych:

Skutki kradzieży danych				
wyciek danych	możliwość przeprowadzenia kolejnych ataków z wykorzystaniem skradzionych danych	konsekwencje prawne	konsekwencje finansowe	utrata reputacji

Metody infekcji				
e-mail zawierający złośliwy załącznik lub link	fałszywa strona WWW (kod złośliwy osadzony na stronie lub plik do pobrania)	nośnik pamięci (np. USB, płyta, itp.)	nielegalne (piracki) oprogramowanie	Atak APT

Dlaczego cyberbezpieczeństwo jest istotne?

Ransomware:

Skutki ataku Ransomware				
utrata dostępu do danych wyciek danych	zakłócenie ciągłości działania organizacji	konsekwencje prawne	konsekwencje finansowe	utrata reputacji

Metody infekcji				
e-mail zawierający złośliwy załącznik lub link	fałszywa strona WWW (kod złośliwy osadzony na stronie lub plik do pobrania)	nośnik pamięci (np. USB, płyta, itp.)	nielegalne (piracki) oprogramowanie	Atak APT

Od czego zacząć..

Od czego zacząć…

INWENTARYZACJA ZASOBÓW
Dane (krytyczne, wrażliwe, osobowe, itp.)
Infrastruktura i zasoby IT (on-premise i chmura)
Wsparcie i serwis
Usługi
Procesy
Ciągłość działania
Podatności
Licencje
Uprawnienia i dostęp
i inne…

Od czego zacząć…

Identyfikacja zagrożeń to proces w którym identyfikujemy potencjalne zagrożenia, odpowiednio je kategoryzujemy, nadajemy im priorytety i wskazujemy środki zaradcze.

Wynikiem identyfikacji zagrożeń **jest odpowiedź na pytania:**

- Gdzie jestem najbardziej podatny na atak?
- Jakie są największa zagrożenia?
- Jak się bronić?

Elementem identyfikacji zagrożeń mogą być

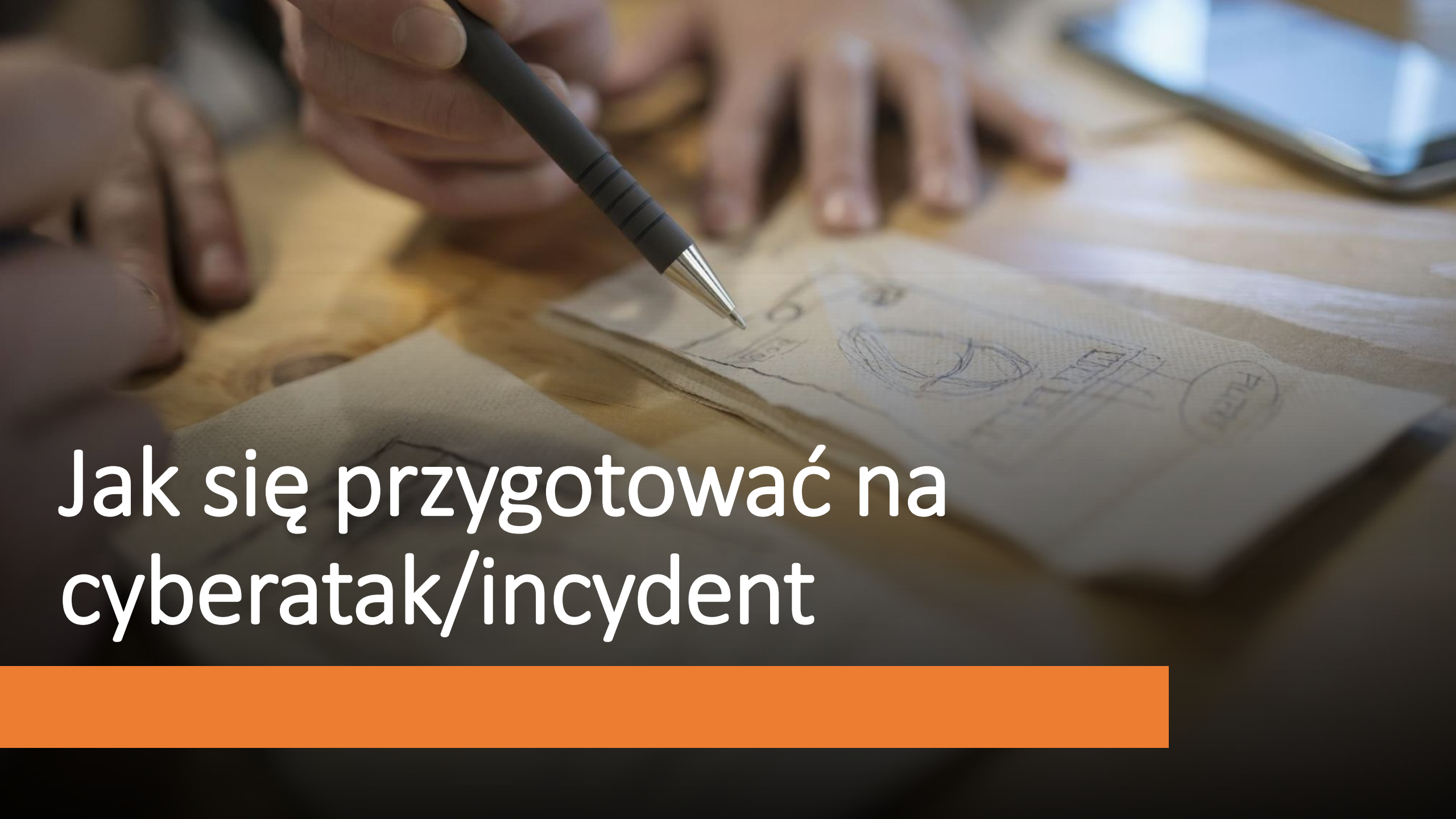
testy penetracyjne

Od czego zacząć…

Dysponując wynikami Inwentaryzacji Zasobów i zidentyfikowanymi Zagrożeniami należy przygotować PLAN DZIAŁANIA

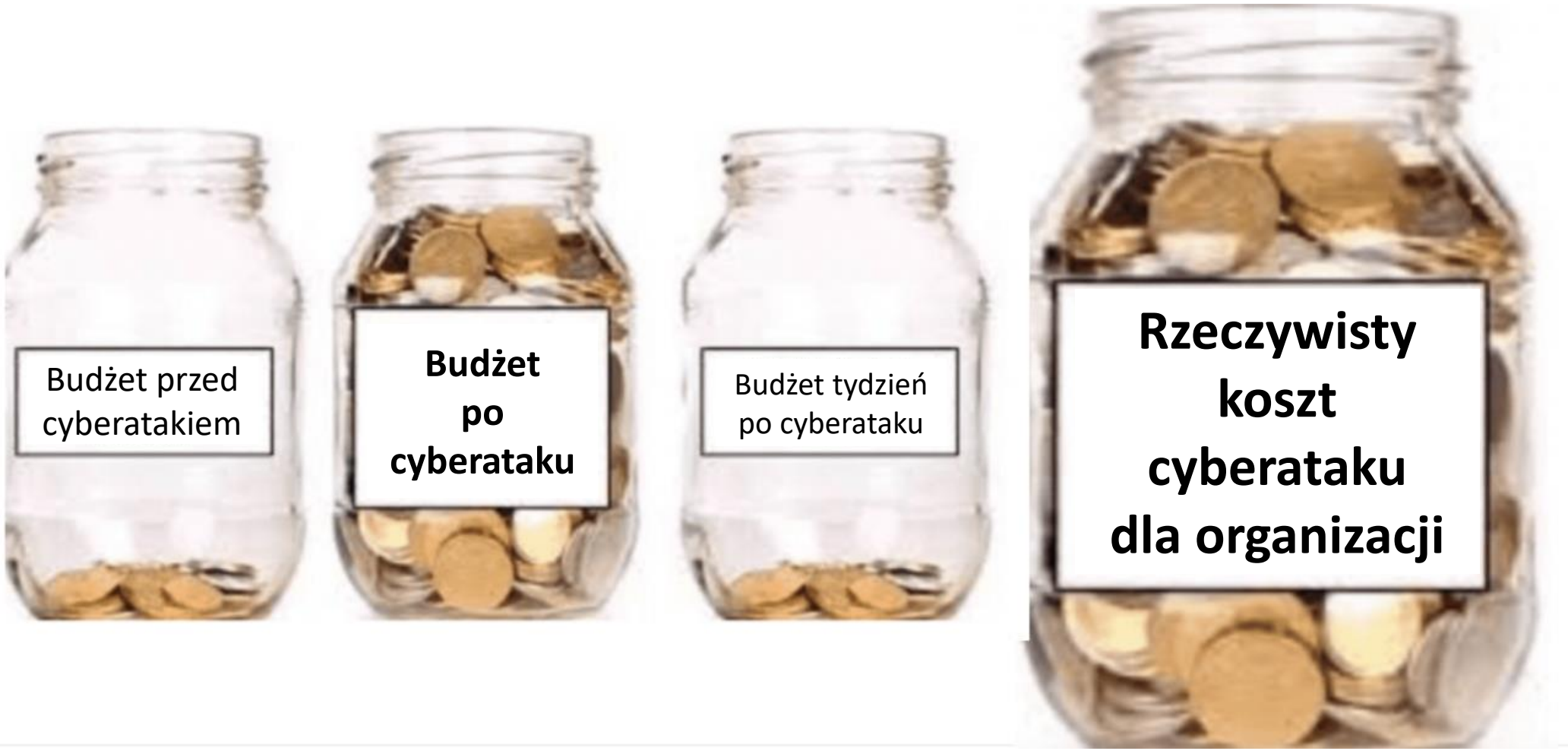
Co taki plan powinien zawierać?

1. Plan likwidacji wykrytych luk i podatności bezpieczeństwa, nie tylko w obszarze infrastruktury, ale także w dziedzinie procedur i procesów
2. Plan ciągłości działania
3. Plan postępowania z incydentem
4. …



Jak się przygotować na cyberatak/incydent

Jak się przygotować na cyberatak/incydent



Jak się przygotować na cyberatak/incydent

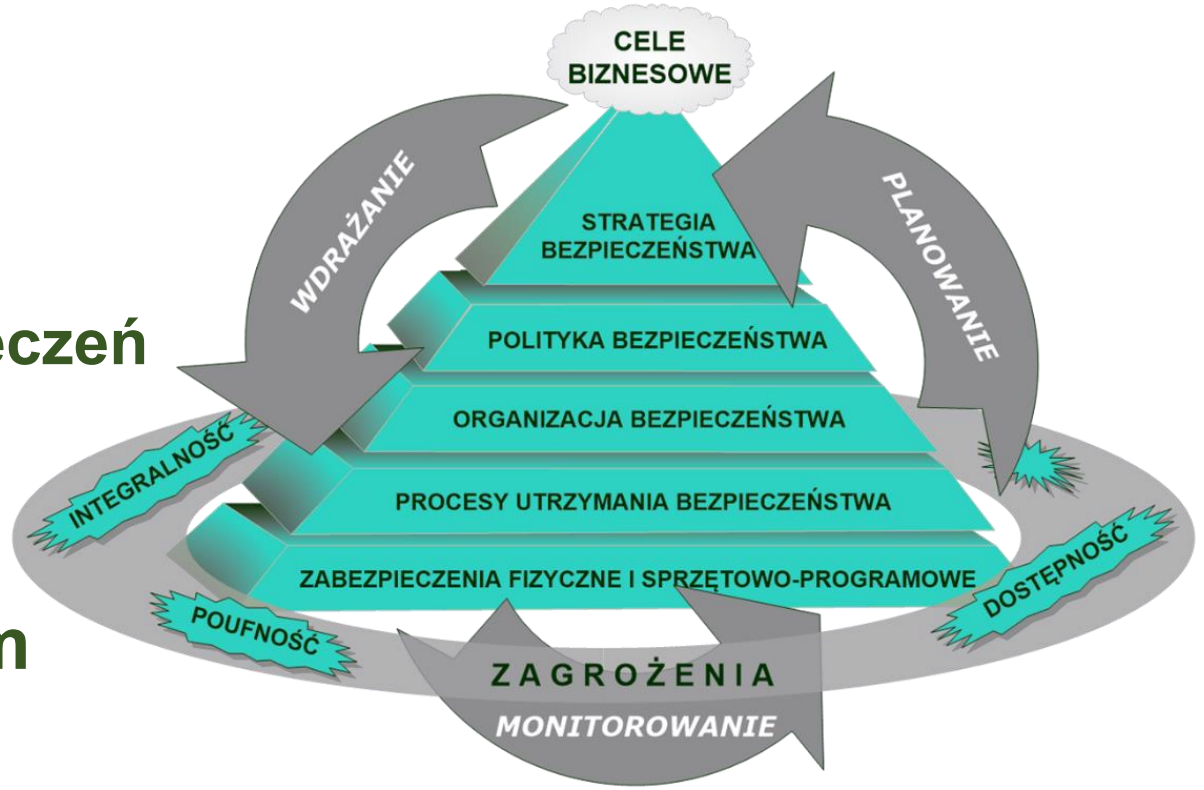
Kompetencje

NAJSKUTECZNIEJSZYM SPOSOBEM OCHRONY PRZED CYBERATAKAMI JEST WYEDUKOWANIE PRACOWNIKÓW W ZAKRESIE PODSTAWOWYCH ZASAD CYBERBEZPIECZEŃSTWA.

Jak się przygotować na cyberatak/incydent

Organizacja i procedury

1. Polityka bezpieczeństwa
   - Procedury backupu
   - Procedury dostępu i uprawnień
   - Procedury monitorowania i zabezpieczeń
   - Odpowiedzialność i inne
2. Plan ciągłości działania
3. Plan postępowania z incydentem
   - Procedury
   - Komunikacja
   - inne



https://www.ican.pl/b/czy-cyberbezpieczenstwo-to-wyzwanie-wylacznie-dla-it-relacja-ze-sniadania-biznesowego-klubu-cfo/P1B0SVk2Z

Jak się przygotować na cyberatak/incydent

Technologia

https://colohouse.com/infographic-defense-in-depth/

Incydent – mleko się rozlało, co dalej…

Incydent – mleko się rozlało, co dalej…

Wykrycie Incydentu

- Raport użytkownika
- Informacja z systemu monitoringu
- Informacja zewnętrzna
- …

Średni czas wykrycia Incydentu (MTTD) to **207 dni***

Kategoryzacja Incydentu

- Klasyfikacja na bazie skutków, skali, zagrożenia dla ciągłości działania, itp.
- Priorytetyzacja incydentu

Odpowiedź na Incydent

- Zdefiniowanie ról i odpowiedzialności członków zespołu reagowania, w zgodzie z procedurami
- Uruchomienie kanałów komunikacji oraz ścieżek decyzyjnych w zgodzie z procedurami

Analiza Incydentu

- Przeprowadzenie analizy w celu identyfikacji przyczyny incydentu
- Przeprowadzenie analizy w celu określenia skali zasięgu incydentu
- Zebranie śladów, logów, danych o incydencie
- Określenie działań (obejść), których wdrożenie ograniczy skutki incydentu

Mitygacja Incydentu

- Uruchomienie niezbędnych zasobów
- Wdrożenie działań ograniczających skutki incydentu

Raportowanie o Incydencie

- Powiadomienie potencjalnie poszkodowanych
- Cykliczne raportowanie postępów prac związanych z obsługą incydentu do osób decyzyjnych
- Cykliczne raporty wewnętrzne i zewnętrzne

Odtworzenie po Incydencie

- Przywrócenie poprawnego funkcjonowania organizacji po incydencie
- Wdrożenie stałych rozwiązań w miejsce obejść przeciwdziałających wystąpieniu incydentu

Wnioski po Incydencie

- Analiza poincydentowa
- Wdrożenie wniosków z analizy
- Zmiana procedur i procesów
- Wdrożenie rozwiązań technologicznych

Średni czas odpowiedzi, analizy i mitygacji Incydentu to**70 dni***

* - Raport IBM „Cost of a data breach 2022” (https://www.ibm.com/reports/data-breach)

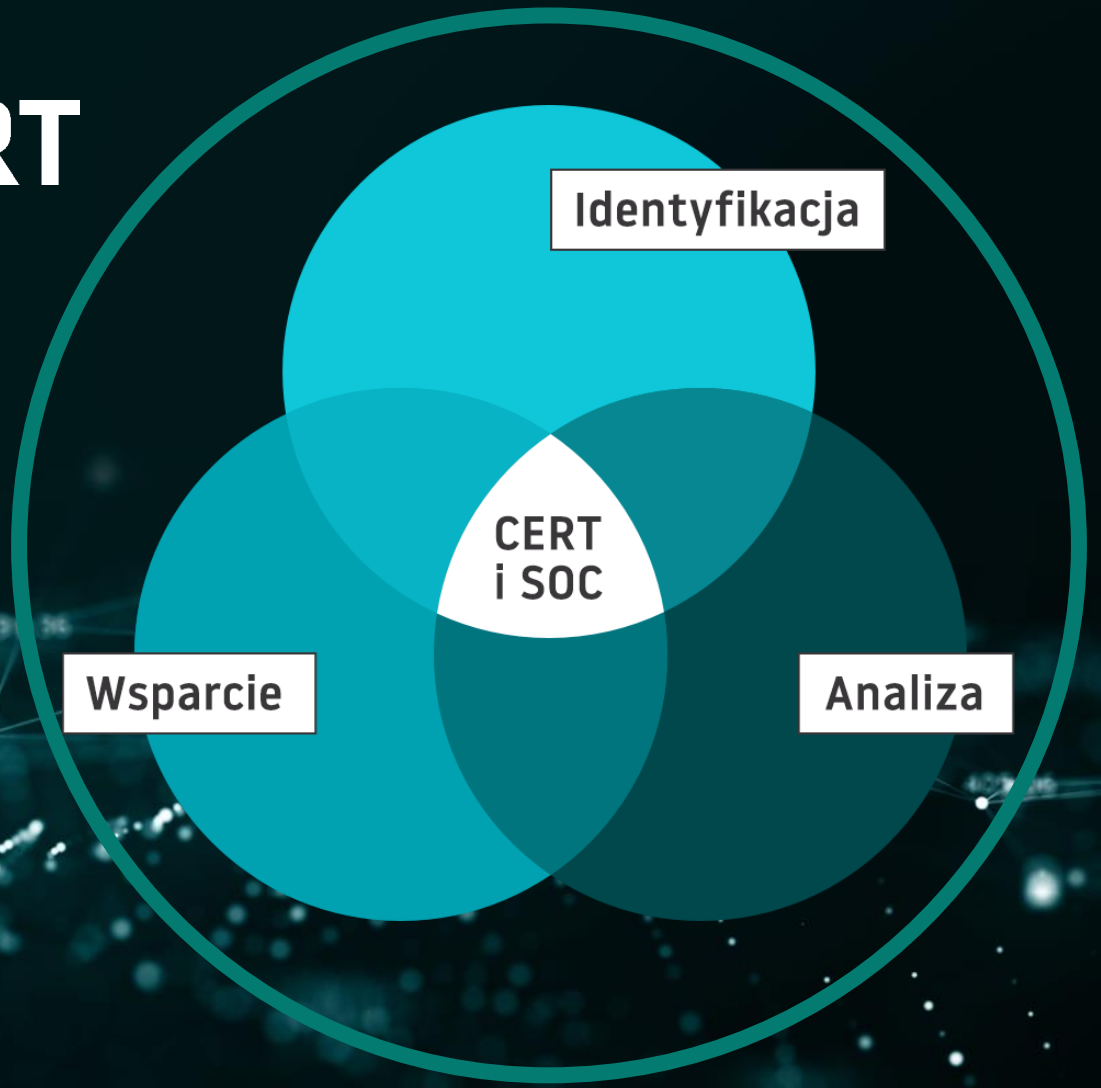
Incydent – mleko się rozlało, co dalej…

1. Postepuj zgodnie z procedurami i instrukcjami
2. Nie panikuj ☺
3. Nie wyciągaj pochopnych wniosków
4. Bądź ostrożny w identyfikacji atakującego
5. Patrz całościowo – oceń pełny zakres incydentu
6. Zrozum interesariuszy, osoby decyzyjne wyższego szczebla i poszkodowanych
7. Stosuj zasady zabezpieczania śladów kryminalistycznych, dokumentuj obsługę incydentu
8. Informuj o postępach
9. Dokładnie oceń wpływ środków i działań zaradczych
10. **Nie bój się prosić o pomoc!!!**

Partner merytoryczny

ComCERT

Koncentrujemy się na usługach określonych jako identyfikowanie zagrożeń i incydentów w cyberprzestrzeni, tworzenie i podnoszenie kompetencji osób i zespołów odpowiedzialnych za cyberbezpieczeństwo (m. in. CERT, SOC) oraz wsparcie Klientów w sytuacjach zagrożenia lub naruszenia ich bezpieczeństwa.



ComCERT dostarcza szeroki zakres produktów i usług w zakresie cyberbezpieczeństwa dla dużych, średnich i małych przedsiębiorstw obejmujący:

- **prewencję** (zabezpieczanie systemów informatycznych przed zagrożeniami) – opartą o integrację systemów cyberbezpieczeństwa oraz doradztwo w zakresie bezpiecznej architektury
- **reakcję** (identyfikację / wykrywanie i zwalczanie / mitygację) zagrożeń i incydentów – opartą o produkty i usługi wsparcia dla zespołów cyberbezpieczeństwa

Ponadto aktywnie uczestniczymy w kształceniu kadr cyberbezpieczeństwa – nasi pracownicy prowadzą wykłady na wielu uczelniach m.in.: Politechnika Warszawska, Wojskowa Akademia Techniczna, Akademia Marynarki Wojennej, Uniwersytet WSB Merito.

Zapraszam do kontaktu

Weronika Marusińska
Polski Fundusz Rozwoju

e-mail: weronika.marusinska@pfr.pl
telefon: +48 511 632 579

PFR
Polski Fundusz Rozwoju

Sieć Firm Przyszłości