PARP Grupa PFR / Centrum Rozwoju MŚP

Cyberbezpieczeństwo w MŚP – ocena ryzyka, zabezpieczenie i ochrona systemów

Marcin Kowalczyk

14.06.2022

PARP Grupa PFR Centrum Rozwoju MŚP

Agenda:

1. Wymagania i standardy cyberbezpieczeństwa w sektorze małych i średnich przedsiębiorstw
2. Zarządzanie Ryzykiem w obszarze cyberbezpieczeństwa
3. Zabezpieczenia i ochrona Infrastruktury Informatycznej
4. Wskazówki i dobre praktyki w codziennej działalności
5. Pytania i odpowiedzi

PARP Grupa PFR / Centrum Rozwoju MŚP

Wymagania i standardy cyberbezpieczeństwa w sektorze małych i średnich przedsiębiorstw

Cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

Zagrożenie cyberbezpieczeństwa – potencjalne działania (człowieka lub sił natury) dotyczące bezpośrednio systemu informacyjnego, mogące spowodować szkody.

PARP Grupa PFR / Centrum Rozwoju MŚP

Wymagania i standardy cyberbezpieczeństwa w sektorze małych i średnich przedsiębiorstw

Dlaczego chronimy informację? Wymagania prawne

Niektóre podstawowe przepisy prawne, nakładające konieczność ochrony informacji to:

- Ustawa o ochronie danych osobowych
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
- Ustawa o krajowym systemie cyberbezpieczeństwa
- Kodeks Pracy
- Ustawa o prawie autorskim i prawach pokrewnych (ochrona własności intelektualnej) - patenty
- Ustawa o rachunkowości (informacje finansowo-księgowe)
- Ustawa o zwalczaniu nieuczciwej konkurencji (tajemnica przedsiębiorstwa)
- Przepisy właściwe dla działalności (np. prawo energetyczne, prawo bankowe, ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, itp.)

PARP Grupa PFR / Centrum Rozwoju MŚP

Wymagania i standardy cyberbezpieczeństwa w sektorze małych i średnich przedsiębiorstw

Dlaczego chronimy informację ?

Informacja jest zasobem i – jak każdy zasób – **posiada swoją wartość. Jest towarem**, którego utrata lub zniszczenie powoduje straty finansowe. Aby zapobiec tego typu stratom konieczna jest jej odpowiednia ochrona.

PARP Grupa PFR / Centrum Rozwoju MŚP

Wymagania i standardy cyberbezpieczeństwa w sektorze małych i średnich przedsiębiorstw

Informacja + Aktywo informacyjne

- ~ komputer
- ~ dysk przenośny
- ~ system informatyczny

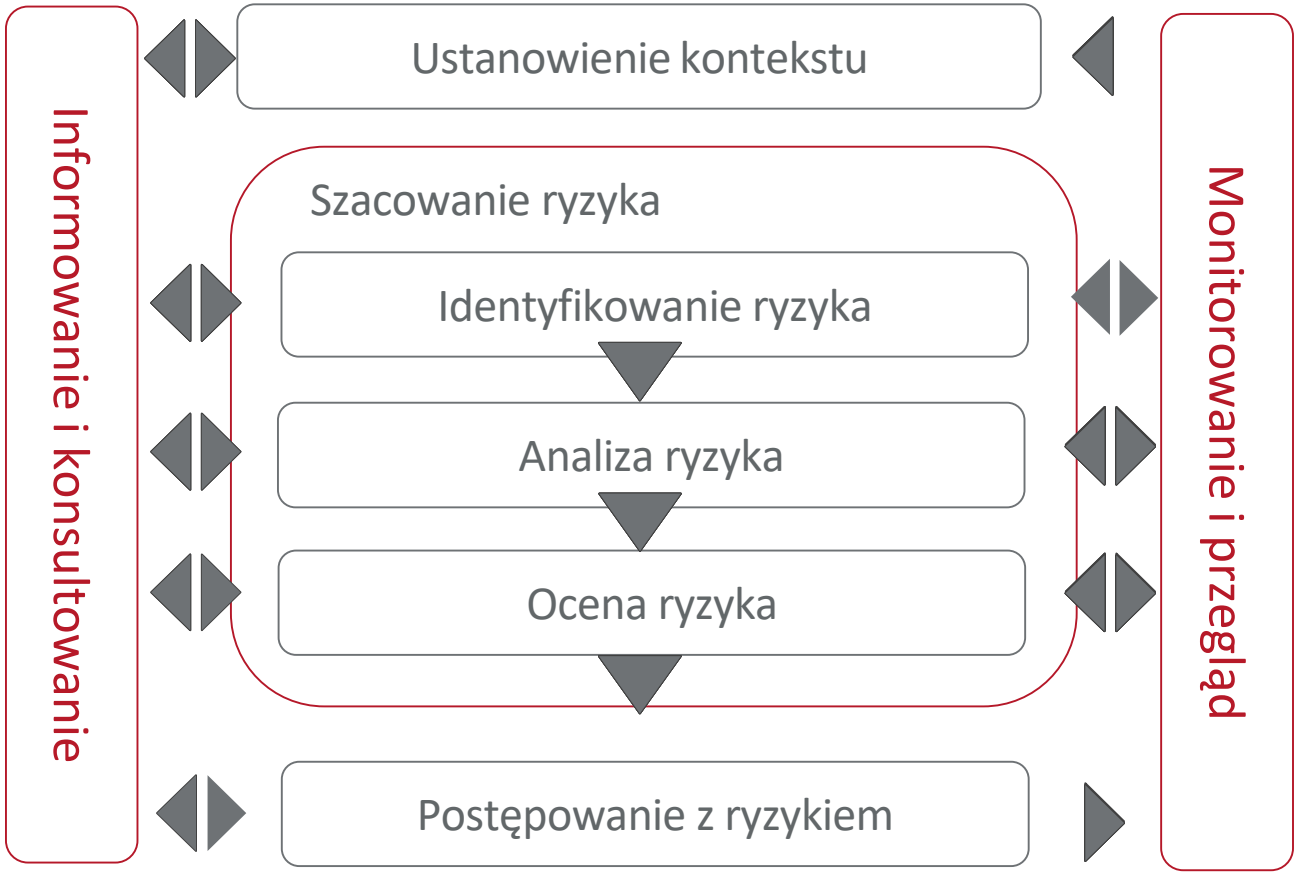
Tworzenie → Przetwarzanie (kopiowanie, edytowanie) Przesyłanie Przechowywanie → Niszczenie

PARP Grupa PFR Centrum Rozwoju MŚP

Wymagania i standardy cyberbezpieczeństwa w sektorze małych i średnich przedsiębiorstw

- ISO/IEC 27001
- ISO/IEC 27002 | ISO/IEC 27017 | ISO/IEC 27032 | ISO/IEC 27034 | ISO/IEC 27035
- Cobit
- NIST CYBERSECURITY FRAMEWORK
- CIS benchmarks
- PCI DSS

Zarządzanie Ryzykiem w obszarze cyberbezpieczeństwa



Zarządzanie Ryzykiem w obszarze cyberbezpieczeństwa

Analiza ryzyka

Na podstawie prawdopodobieństwa i efektu określany jest poziom ryzyka, który służy pomocą przy klasyfikacji ryzyk.

W uproszczeniu poziom ryzyka otrzymujemy poprzez zestawienie prawdopodobieństwa ze skutkami wystąpienia danego zdarzenia:

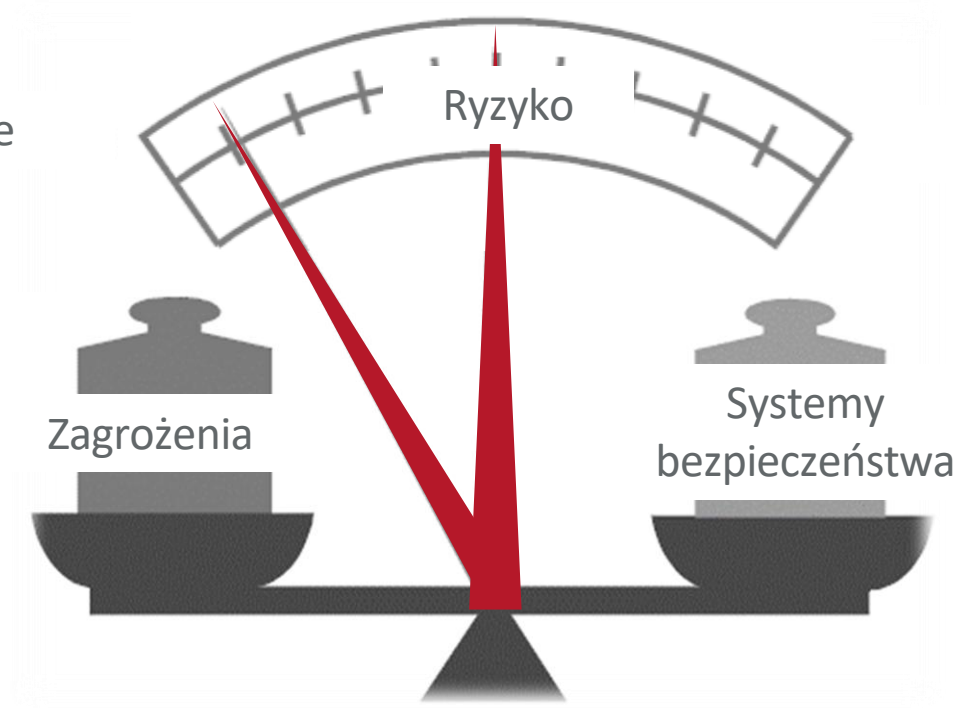
Prawdopodobieństwo × Skutek → Poziom ryzyka

Przy czym należy wziąć pod uwagę istniejące techniki postępowania z ryzykiem – środki kontroli ryzyka oraz ich skuteczność.

Zarządzanie Ryzykiem w obszarze cyberbezpieczeństwa

Ryzyko nieakceptowalne

Zdolność do powodowania strat



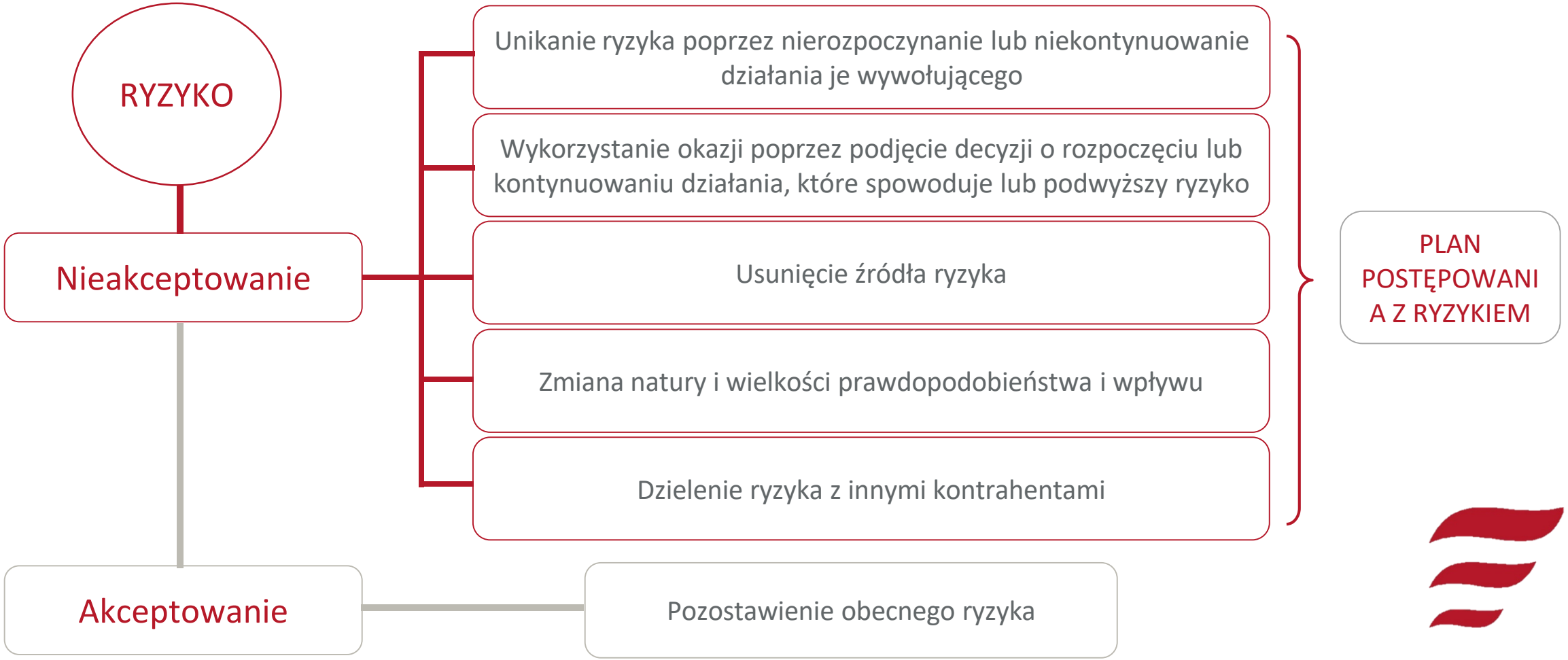
Ryzyko akceptowalne

Zdolność do zapobiegania stratom

Wzajemna relacja między rzeczywistymi zagrożeniami a systemami bezpieczeństwa reprezentującymi odpowiedni poziom ryzyka dla każdej instalacji.

PARP Grupa PFR / Centrum Rozwoju MŚP

Zarządzanie Ryzykiem w obszarze cyberbezpieczeństwa



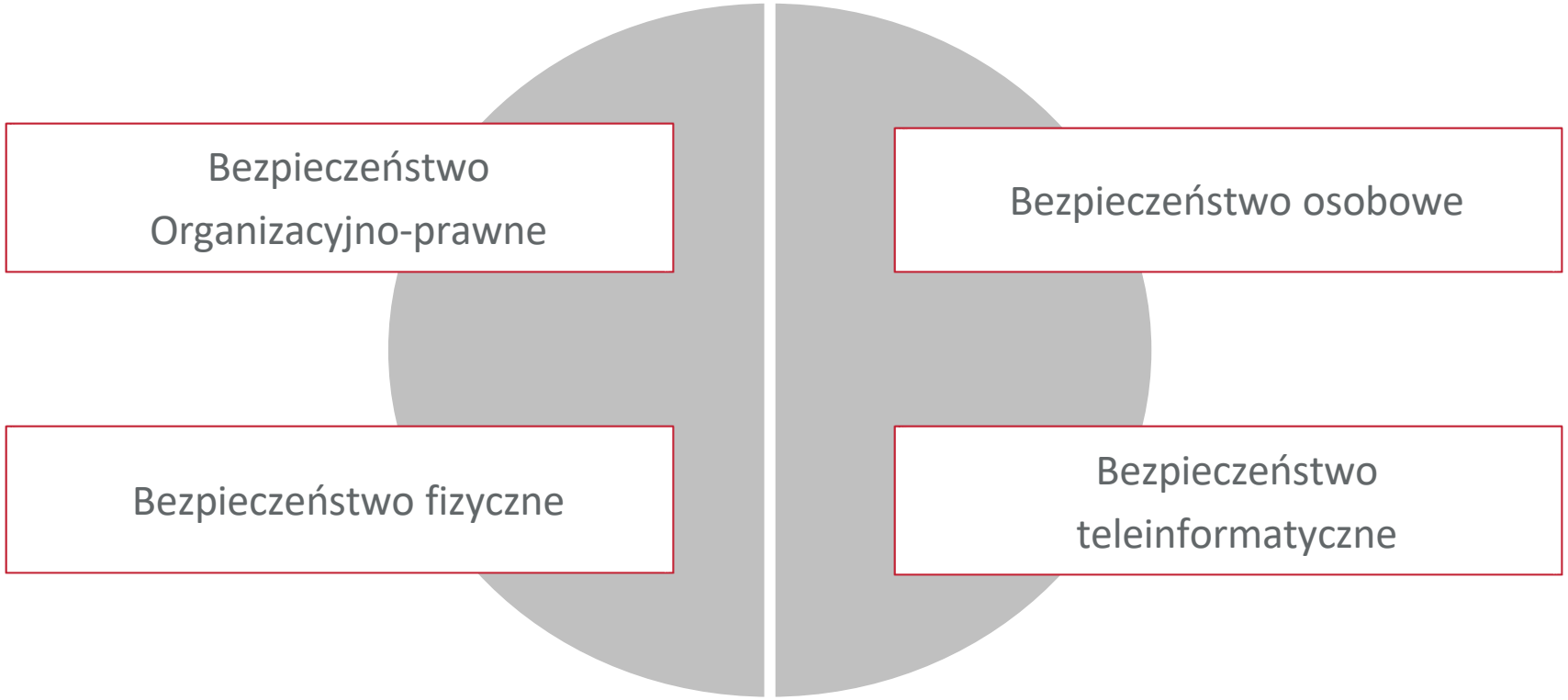
PARP Grupa PFR Centrum Rozwoju MŚP

Zarządzanie Ryzykiem w obszarze cyberbezpieczeństwa

- Testy socjotechnicze
- Testy penetracyjne
- Analiza konfiguracji Infrastruktury IT
- Stopień wdrożenia zabezpieczeń
- Audyty wewnetrzne lub zewnętrzne
- Incydenty bezpieczeństwa

Zabezpieczenia i ochrona Infrastruktury Informatycznej

System obejmuje strukturę organizacyjną, polityki, działania planistyczne, zakresy odpowiedzialności, praktyki, procedury, procesy i zasoby.



PARP Grupa PFR / Centrum Rozwoju MŚP

Zabezpieczenia i ochrona Infrastruktury Informatycznej

- Zarządzanie ryzykiem
- Zarządzanie ciągłością działania
- Zarządzanie incydentami
- Zarządzanie podatnościami
- Zarządzanie zmianami
- Zarządzanie dostępem
- Zarządzanie pojemnością
- Zarządzanie projektami
- Zarządzanie aktywami
- Zarządzanie zgodnością (compliance)
- Nadzór nad dokumentacją
- Bezpieczeństwo informacji w relacjach z dostawcami
- Bezpieczeństwo fizyczne
- Bezpieczeństwo osobowe
- Bezpieczna eksploatacja
- Pozyskiwanie, rozwój i utrzymanie systemów
- Monitorowanie, audyt i testowanie

PARP Grupa PFR Centrum Rozwoju MŚP

Zabezpieczenia i ochrona Infrastruktury Informatycznej

Monitorowanie cyberbezpieczeństwa

Posiadanie zdolności do ciągłego monitorowania systemu informacyjnego, w szczególności zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach.

Systemy informatyczne:

- właściwy nadzór operatorski (użytkowników)
- właściwy nadzór administracyjny
- systemy informatyczne:
  - Firewall
  - klasy SIEM
  - skanery podatności
  - klasy DLP
  - zaawansowana analityka IT/OT

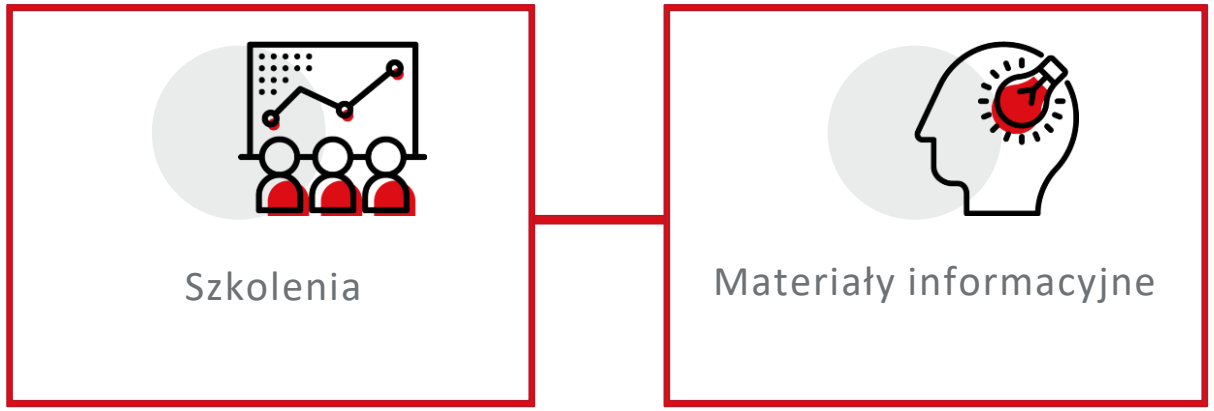
Ataki na systemy it

Cyberatak w większości przypadków jest tak naprawdę działaniem wymierzonym w pojedynczego użytkownika

- Spam
- Skanowanie sieci, portów (scanning)
- Podsłuch informacji (sniffing)
- Podszywanie się (spoofing)
- Ataki typu Man – in – the – Middle
- Outsourcing
- Błędy programistyczne
- Błędy w konfiguracji
- Złośliwe oprogramowanie (malware)
- Odmowa wykonania usługi (DoS, DDoS)
- Ataki na sieci WiFi

PARP Grupa PFR / Centrum Rozwoju MŚP

Bardzo ważnym elementem cyberbezpieczeństwa jest świadomość



PARP Grupa PFR / Centrum Rozwoju MŚP

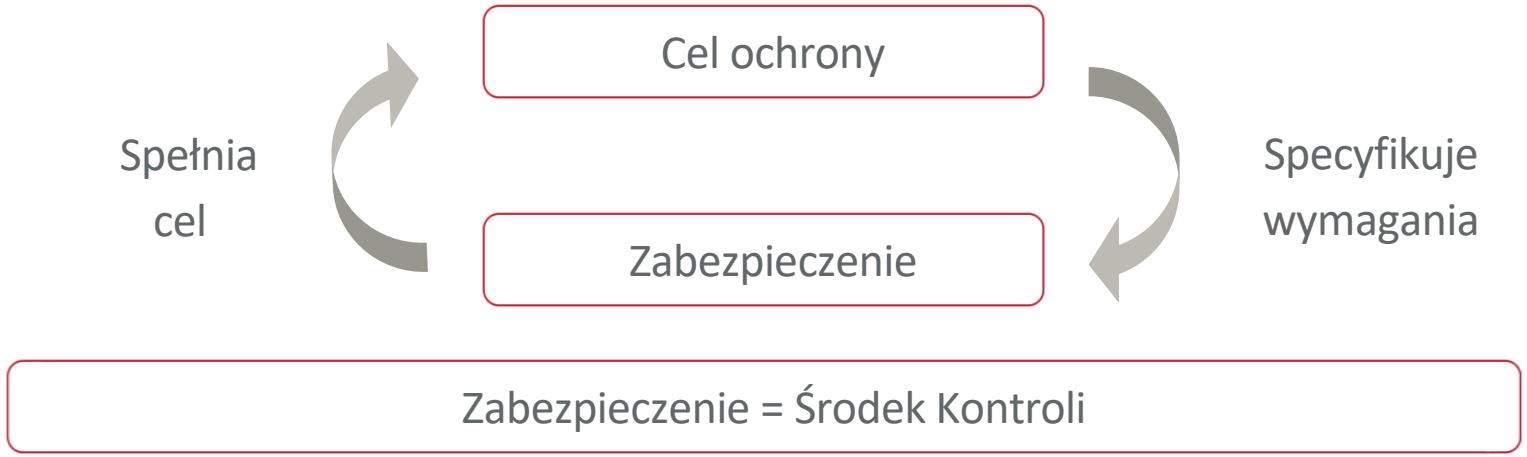
Wskazówki i dobre praktyki w codziennej działalności

Wymagania normy ISO 27001 – załącznik A

Zabezpieczenia – Załącznik A

- Załącznik A został podzielony na 14 obszarów zabezpieczeń
- W każdym obszarze zgrupowano kilka celów zabezpieczeń
- Dla każdego celu określono zabezpieczenia
- Sprecyzowano w sumie 114 zabezpieczeń

Efektywne zabezpieczenie?!



PARP Grupa PFR / Centrum Rozwoju MŚP

Bezpieczeństwo Komunikacji

Polityka Bezpieczeństwa Informacji

Relacja z Dostawcami

Zarządzanie aktywami

Kryptografia

Kontrola Dostępu

Zgodność

Bezpieczeństwo Fizyczne i Środowiskowe

Zarządzanie Incydentami Bezpieczeństwa

Ciągłość Działania

Bezpieczeństwo Zasobów Ludzkich

Organizacja Bezpieczeństwa Informacji

Pozyskiwanie, Rozwój i Utrzymanie Systemów

Bezpieczna Eksploatacja

Wdrożenie

Stosowanie polityk I zasad

Opracowanie dokumentacji

Sformalizowanie polityk, procedór I zasad bezpieczeństwa informacji

Analiza ryzyka

Dobór adekwatnych zabezpieczeń

Audyt

Określenie miejsca w którym jesteśmy

SZBI to nie jest wyłącznie:

- bezpieczne oprogramowanie
- bezpieczny sprzęt i urządzenia
- bezpieczna infrastruktura
- procedury i regulacje prawne
- świadomość pracowników
- wybrane zagadnienie z powyższych

SZBI jest gwarantem najwyższych standardów bezpieczeństwa informacji tylko i wyłącznie jeżeli podejdziemy do tego w sposób całościowy, czyli uwzględnimy wszystkie powyżej opisane aspekty bezpieczeństwa!

PARP Grupa PFR Centrum Rozwoju MŚP

Kontakt:

Tomasz Borkowski

PBSG

tel.: +48 511 896 845

e-mail: tomasz.borkowski@pbsg.pl

www.pbsg.pl