Co-funded by the Erasmus+ Programme of the European Union

Moduł treningowy InCyT

Bezpieczeństwo informacji dla menedżerów **Część 4, Tydzień 7 i 8** **Moduł: Ryzyko i odporność w cyberprzestrzeni**	
Zajęcia edukacyjne	❑ **Webinaria** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑ **Prezentacja** ❑ **Inne**
Odpowiedzialni za zajęcia	• Simon Tjoa • Peter Kieseberg
Cele aktywności edukacyjnej	1. Uczestnicy znają podstawy zarządzania ryzykiem i odpornością. 2. Uczestnicy potrafią przeprowadzić analizę wpływu na biznes i analizę ryzyka 3. Uczestnicy potrafią wyprowadzić z wyników analiz środki zaradcze i decyzje dotyczące bezpieczeństwa
Umiejętności do zdobycia	• IS 1, IS 3 • MS 1
Czas trwania okresu edukacyjnego	2 tygodnie • Tydzień 7 (2 godziny) • Tydzień 8 (2 godziny)
Wymagania wstępne	***Co jest potrzebne?***
	• Podstawowe umiejętności w zakresie zarządzania • Podstawowe umiejętności informatyczne • Podstawowe umiejętności w zakresie bezpieczeństwa

Co-funded by the Erasmus+ Programme of the European Union

Krótka informacja o module

Opis
Idealne bezpieczeństwo nie jest możliwe. Wiedząc o tym, należy podejmować świadome decyzje, jak wydawać pieniądze na właściwe środki bezpieczeństwa. Zarządzanie ryzykiem cybernetycznym i odpornością na nie dostarcza istotnego zestawu narzędzi i technik do oceny aktualnego stanu bezpieczeństwa organizacji oraz planowania kontroli w celu utrzymania ryzyka bezpieczeństwa informacji na akceptowalnym poziomie.

Treść materiałów dydaktycznych

Bez podejmowania ryzyka prowadzenie działalności gospodarczej jest niemożliwe. Dlatego zarządzanie ryzykiem oraz odpowiednie narzędzia i techniki zapewniają systematyczny sposób podejścia do ryzyka. Zarządzanie ryzykiem pozwala odpowiedzieć na pytania, jak duże bezpieczeństwo jest wystarczające lub który środek zaradczy powinien być wdrożony w pierwszej kolejności. Dlatego też zarządzanie ryzykiem jest ważnym działaniem umożliwiającym podejmowanie świadomych decyzji. Ważne normy i najlepsze praktyki dotyczące tego istotnego tematu obejmują ISO 27005, ISO 31000 lub BSI 200-3.

Zanim przyjrzymy się bliżej procesowi zarządzania ryzykiem, należy zdefiniować istotne pojęcia:

- **Podatność**: "Słabość w systemie informatycznym, procedurach bezpieczeństwa systemu, kontrolach wewnętrznych lub luka, która może zostać wykorzystana lub wywołana przez źródło zagrożenia[1]
- **Kontrola**: "Zabezpieczenie lub środek zaradczy zalecany dla systemu informacyjnego lub organizacji zaprojektowany w celu ochrony poufności, integralności i dostępności jego informacji oraz spełnienia zestawu zdefiniowanych wymagań bezpieczeństwa"[2]
- **Zagrożenie**: "Każda okoliczność lub zdarzenie, które może mieć negatywny wpływ na operacje organizacyjne (w tym misję, funkcje, wizerunek lub reputację), aktywa organizacyjne, osoby, inne organizacje lub naród (mieszkańców) za pośrednictwem systemu informacyjnego poprzez nieuprawniony dostęp, zniszczenie, ujawnienie, modyfikację informacji i/lub odmowę usługi. "[3]

[1] https://csrc.nist.gov/glossary/term/vulnerability
[2] https://csrc.nist.gov/glossary/term/security_control
[3] https://csrc.nist.gov/glossary/term/threat

- **Ryzyko**: "Miara stopnia, w jakim jednostka jest zagrożona przez potencjalne okoliczności lub zdarzenie i zazwyczaj jest funkcją: (i) niekorzystnego wpływu, czyli wielkości szkody, która powstałaby w przypadku wystąpienia okoliczności lub zdarzenia oraz (ii) prawdopodobieństwa wystąpienia." [4]

Z definicji ISO 31000 ("efekt niepewności"[5]) możemy wywnioskować, że ryzyka mogą mieć pozytywne i negatywne skutki. Często, jeśli ryzyka mają pozytywne skutki, są określane jako szanse.

Ogólny proces zarządzania ryzykiem rozpoczyna się od określenia zakresu, kontekstu i kryteriów. Ponieważ nie wszystkie ryzyka dotyczące wszystkich działań mogą być analizowane, ważne jest ustalenie priorytetów i podjęcie decyzji, które usługi, procesy i jednostki organizacyjne powinny być objęte oceną. Posiadanie odpowiedniego zakresu jest kluczowe dla zapewnienia ważnych wyników z jednej strony i rozsądnego wysiłku z drugiej. Kontekst to środowisko wewnętrzne i zewnętrzne. Określenie kryteriów ryzyka jest ważne dla zapewnienia powtarzalnego procesu, który prowadzi do porównywalnych wyników. Kryteria powinny być zdefiniowane w taki sposób, aby różne osoby były w stanie ocenić ryzyko we wspólny sposób.

Przykłady kryteriów obejmują kryteria wpływu (np. niski, średni, wysoki) dla różnych wymiarów, takich jak finansowy, reputacja czy zdrowie.

W dalszej części przedstawiono przykład OCTAVE Allegro dotyczący reputacji i wpływu na klienta:

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Rysunek 1: Kryteria pomiaru reputacji [6]

Po zdefiniowaniu kryteriów i zakresu ryzyka, pierwszym krokiem jest identyfikacja ryzyka. Identyfikacja ryzyka jest kluczowa, ponieważ tylko te ryzyko może być ocenione, które zostało

[4] https://csrc.nist.gov/glossary/term/risk
[5] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[6] https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf

zidentyfikowane. Dlatego sensowne jest porównanie zidentyfikowanych zagrożeń z listami zagrożeń ISO 27005, MEHARI lub innych najlepszych praktyk lub standardów.

Istnieją różne techniki identyfikacji ryzyka[7], takie jak burza mózgów, technika Delphi, Failure Mode and Effects Analysis (FMEA) czy Hazard and Operability Studies (HAZOP).

W kolejnym etapie analizy ryzyka uzyskuje się lepsze zrozumienie zidentyfikowanego ryzyka. W związku z tym określa się prawdopodobieństwo/częstotliwość wystąpienia oraz wpływ/konsekwencje. W celu określenia konsekwencji ważne jest zdefiniowanie systematycznego sposobu oceny wpływu. Często łatwiej jest zastosować miarę jakościową (np. niski, średni, wysoki) niż miarę ilościową.

Ryzyko jest często wizualizowane w tzw. matrycy ryzyka, która podkreśla ryzyko używając prawdopodobieństwa i wpływu jako osi.

Probability	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Rysunek 2: Macierz ryzyka [Źródło Wikipedia] [8]

W kolejnym kroku ryzyko jest oceniane. Oznacza to, że wyniki poprzedniego kroku są brane pod uwagę w celu podjęcia decyzji, czy należy podjąć działania. Ponadto, dokonuje się priorytetyzacji ryzyka.

Następnie określana jest jedna z czterech głównych strategii przeciwdziałania ryzyku:

- Akceptacja ryzyka: dokumentowanie i monitorowanie ryzyka, jeśli ryzyko mieści się w ramach zakresu akceptacji organizacji
- Transfer ryzyka: dzielenie się ryzykiem (np. ubezpieczenie, wspólne przedsięwzięcia)
- Unikanie ryzyka: usunięcie źródła ryzyka

[7] Cmp. https://www.iso.org/standard/72140.html
[8] https://en.wikipedia.org/wiki/Risk_matrix

- Łagodzenie ryzyka: zmniejszenie wpływu lub prawdopodobieństwa wystąpienia (np. kontrola dostępu)

Po określeniu środków zaradczych ocenia się, czy ryzyko, także szczątkowe jest do przyjęcia, czy też należy podjąć dalsze środki.

Jako działania wspierające obok głównego procesu oceny ryzyka, odbywa się także komunikacja o ryzyku (tj. komunikacja z odpowiednim interesariuszem), monitorowanie ryzyka oraz raportowanie o ryzyku.

Ponieważ nie wszystkie ryzyka mogą być brane pod uwagę, w przeciwieństwie do zarządzania ryzykiem, ciągłość "działania i odporności" skupia się na krytycznych działaniach zamiast na poszczególnych ryzykach. W ten sposób możliwe jest przygotowanie się na nieznane i mało prawdopodobne/wysokie ryzyko.

Dla zapewnienia skutecznego programu ciągłości działania niezbędne jest wsparcie najwyższego kierownictwa. Ważnym aspektem podkreślającym znaczenie zarządzania ciągłością działania jest polityka ciągłości działania. W tym dokumencie kierownictwo wyraża formalnie swoje poparcie. Ponadto, dokument ten podkreśla zakres i cele działań związanych z ciągłością działania, ważne role i obowiązki (np. kierownik ds. ciągłości działania), jak również ramy operacyjne wykorzystywane do realizacji programu. Należy podkreślić, że zakres nie powinien być zbyt szeroki, aby zapewnić, że złożoność analizy oraz wysiłek nie staną się zbyt duże.

W celu zrozumienia wpływu zakłóceń w świadczeniu usług na biznes oraz uzyskania dobrej podstawy do planowania działań naprawczych przeprowadza się analizę wpływu na biznes. Jest to centralne narzędzie w procesie ciągłości działania i pozwala uchwycić istotność oraz znaczenie produktów I usług. Oprócz krytyczności produktów oraz usług określane i oceniane są ich zależności.

Do ważnych kluczowych wartości, które są wykorzystywane podczas przeprowadzania analizy wpływu na biznes należą:

- **MAO (maksymalna dopuszczalna przerwa w pracy,** ang. ***maximum acceptable outage*****)**: "czas, jaki byłby potrzebny, aby negatywne skutki [...], które mogą powstać w wyniku niedostarczenia produktu/usługi lub niewykonania czynności [...], stały się nieakceptowalne".[9]
- **RTO (czas odzyskiwania,** ang. ***recovery time objective*****):** "okres czasu po incydencie [...], w którym produkt i usługa [...] lub działalność [...] są wznowione, lub zasoby [...] są odzyskane"[10]
- **RPO (punkt odzyskiwania,** ang. ***recovery point objective*****):** "punkt, do którego przywracane

[9] MAO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[10] RTO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

są informacje [...] wykorzystywane przez daną działalność [...], aby umożliwić jej działanie po wznowieniu"[11]

W pierwszym kroku identyfikowane są najbardziej krytyczne lub niezbędne produkty i usługi. Po dokonaniu identyfikacji ocenia się, jakie szkody powstałyby w czasie, gdyby doszło do zakłócenia lub przerwania pracy określonego produktu lub usługi.

Kolejny rysunek pokazuje, jak upływ czasu wpływa na poszczególne kategorie.

Assessment Period / Damage Category	1 Hour(s)	2 Hour(s)	4 Hour(s)	8 Hour(s)	24 Hour(s)	48 Hour(s)	96 Hour(s)	168 Hour(s)	240 Hour(s)	720 Hour(s)
Financial	0	0	0	0	0	0	2	3	4	4
Health & Safety	0	0	0	0	0	0	0	3	4	4
Legal, Regulatory & Contractual	0	0	0	0	1	1	1	2	2	2
Brand and Reputation	0	0	0	1	1	1	2	4	4	4
Environmental	0	0	0	0	0	0	0	0	0	0
Rational for the assessment (Description) Verbal Description of Implications										

Ponadto analiza wpływu na biznes bada, od jakich procesów, działań i zasobów zależą odpowiednie usługi. W ten sposób można określić ważne wartości kluczowe, takie jak czas odzyskiwania, punkt odzyskiwania i maksymalna dopuszczalna przerwa w pracy.

Po poznaniu krytyczności procesów, usług i zasobów opracowywane są strategie ciągłości działania. Strategie te obejmują m.in. dywersyfikację (np. działania w geograficznie oddalonych miejscach), replikację (np. kopiowanie danych w celu ich odtworzenia w innym miejscu) czy podwykonawstwo (np. korzystanie z usług firm trzecich).

Na podstawie tych strategii tworzone są plany ciągłości działania, które wspierają organizacje w skutecznym reagowaniu po wystąpieniu incydentu. Aby plany mogły być użyteczne w sytuacjach wysokiej presji, muszą być odpowiednio napisane. Oznacza to, że plany powinny zawierać tylko te informacje, które są istotne podczas obsługi zdarzenia. Ponadto informacje te powinny być szybko przyswajalne. Dlatego należy stosować przejrzyste i zorientowane na działanie listy kontrolne.

Standardowe plany ciągłości działania zawierają informacje o celu, zakresie, strukturze zarządzania incydentami, rolach i odpowiedzialności, aktywacji planu, ustaleniach dotyczących odtwarzania oraz

[11] RPO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

danych kontaktowych.

W celu przećwiczenia i sprawdzenia adekwatności planów stosuje się różne rodzaje ćwiczeń. Mogą to być zarówno ćwiczenia oparte na dyskusji, takie jak pytania kontrolne przy biurku lub ćwiczenia praktyczne takie jak testowanie przywracania określonych systemów.

Pytania:

Zobacz dokumenty Word

Załączniki:

Zobacz pliki Powerpoint i Video

Referencje:

- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO/TS 22317:2021, Security and resilience — Business continuity management systems — Guidelines for business impact analysis
- ISO/TS 22331:2018, Security and resilience — Business continuity management systems — Guidelines for business continuity strategy
- ISO/TS 22332:2021, Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures
- ISO 31000:2018, Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- IEC 31010:2019, Risk management — Risk assessment techniques