Najczęściej zadawane pytania

1. Co to jest planowanie awaryjne systemu informatycznego?

Planowanie awaryjne systemu informacyjnego odnosi się do dynamicznego rozwoju skoordynowanej strategii odzyskiwania systemów informatycznych, operacji i danych po wystąpieniu zakłócenia. Proces planowania wymaga siedmiu kroków: opracowania deklaracji dotyczącej polityki planowania awaryjnego; przeprowadzenia analizy wpływu na działalność (BIA); zidentyfikowania zabezpieczeń; opracowania strategii odzyskiwania; opracowania planu awaryjnego dla systemu informatycznego (ISCP); przetestowania wykonalności planu i przeszkolenia personel; utrzymywania planu w aktualności.

2. Jakie są różnice między planem zachowania ciągłości operacyjnej (Continuity of Operations Plan – COOP), planem ciągłości działalnia (Business Continuity Plan – BCP), planem ochrony infrastruktury krytycznej (Critical Infrastructure Protection – CIP), planem odzyskiwania po katastrofie (Disaster Recovery Plan – DRP), planem awaryjnym systemu informatycznego (Information System Contingency Plan – ISCP), planem reagowania na incydenty cyberbezpieczeństwa (Cyber Incident Response Plan - CIRP) oraz planem ewakuacyjnym (Occupant Emergency Plan – OEP)?

Organizacje wymagają zestawu planów, aby przygotować się na reakcję, ciągłość, odzyskiwanie i wznawianie procesów biznesowych i systemów informatycznych w przypadku wystąpienia zakłócenia. Każdy plan ma określony cel i zakres; jednak z powodu braku standardowych definicji dla tego rodzaju planów, w niektórych przypadkach zakres rzeczywistych planów opracowanych przez organizacje może różnić się od następujących podstawowych opisów.

COOP jest wymagany w celu utrzymania podstawowych funkcji celu działania organizacji (*ang. Mission Eessential Functions – MEF*) w alternatywnym miejscu i wykonywanie tych funkcji przez 30 dni przed powrotem do normalnej pracy.

BCP odnosi się do podtrzymywania procesów biznesowych oraz systemów informatycznych, które wspierają te procesy biznesowe podczas i po znacznych zakłóceniach. BCP są często opracowywane na poziomie organizacji lub dla procesów biznesowych, które nie są traktowane priorytetowo jako niezbędne.

Plan CIP to zestaw polityk i procedur, które służą do ochrony i odzyskiwania tych elementów infrastruktury krajowej, które są uważane za tak istotne, że ich utrata miałaby wyniszczający wpływ na bezpieczeństwo, ekonomię państwa lub życie i zdrowie obywateli.

DRP odnosi się do planu skoncentrowanego na systemie informatycznym, zaprojektowanego w celu przywrócenia działania jednego lub większej liczby systemów

informacyjnych w alternatywnej lokalizacji po poważnych zakłóceniach, zwykle powodujących fizyczne uszkodzenie pierwotnego centrum danych.

ISCP zapewnia procedury odzyskiwania i wznawiania dla pojedynczego systemu informatycznego, wynikające z zakłóceń, które niekoniecznie wymagają przeniesienia do innej lokalizacji.

CIRP ustanawia procedury umożliwiające pracownikom cyberbezpieczeństwa identyfikację, złagodzenie i odzyskanie zdolności do działania po cyberatakach na systemy informatyczne organizacji.

OEP zapewnia wskazówki osobom przebywającym w obiekcie w przypadku sytuacji awaryjnej zagrażającej zdrowiu i życiu personelu lub szkodom w środowisku lub zniszczeniem mienia.

Należy zachować staranną koordynację między twórcami planów, aby ich wzajemne zasady i procedury się uzupełniały, albo nie były sprzeczne. Wszelkie zmiany w jednym planie, systemie lub procesie muszą być przekazywane planistom powiązanych systemów i funkcji.

3. Jaka jest różnica między procesami biznesowymi obsługiwanymi przez system informatyczny, a kluczowymi funkcjami działania Planu kontynuacji operacji (*ang. Continuity of Operations Plan Mission Essential Function - COOP MEF*)?

Systemy informatyczne są projektowane i rozwijane w celu wspierania procesów / funkcji biznesowych. Podczas przeprowadzania BIA procesy biznesowe są identyfikowane i poddawane priorytetyzacji pod względem krytyczności. COOP MEF to zestaw priorytetowych procesów biznesowych, które wspierają misję organizacji i muszą zostać podjęte w ciągu 12 godzin i utrzymywane do 30 dni. COOP obejmuje szerszy zakres działalności organizacji niż tylko procesy, które są wspierane przez systemy informatyczne. Jednak z uwagi na to, że niektóre procesy biznesowe COOP MEF muszą być wspierane przez systemy informatyczne, dla tych systemów należy opracować ISCP.

4. Jaki jest związek między ramami zarządzania ryzykiem, a planowaniem awaryjnym systemu informatycznego?

Ramy zarządzania ryzykiem (*ang. Risk Management Framework – RMF*) obejmują szeroki zakres działań mających na celu identyfikację, kontrolowanie i ograniczanie ryzyka dla systemu informatycznego podczas cyklu życia systemu. Jednym z działań jest opracowanie ISCP. Wdrożenie ram zarządzania ryzykiem może zapobiegać zagrożeniom naturalnym, ludzkim i środowiskowym lub je zmniejszać, a także ograniczać konsekwencje ryzyka w przypadku zakłócenia systemu.

5. Jak zarządzanie ryzykiem i planowanie awaryjne systemu informacyjnego wpisują się w program odporności?

Celem odpornej organizacji jest ciągłe funkcjonowanie przez cały czas podczas każdego rodzaju zakłócenia. Odporne organizacje nieustannie pracują nad dostosowaniem się do zmian i ryzyka, które mogą wpłynąć na ich zdolność do utrzymania ciągłości działalności. Zarządzanie ryzykiem, planowanie awaryjne i planowanie ciągłości to indywidualne działania w zakresie bezpieczeństwa i zarządzania kryzysowego, które mogą być realizowane w sposób holistyczny w całej organizacji jako elementy programu odporności.

6. Na jakim etapie cyklu życia systemu (*System Development Life Cycle – SDLC)* należy uwzględnić planowanie awaryjne i powiązane środki bezpieczeństwa?

Chociaż planowanie awaryjne jest powiązane z działaniami występującymi w fazie eksploatacji / utrzymania systemu, środki awaryjne powinny być zidentyfikowane i zintegrowane we **WSZYSTKICH** fazach SDLC. Włączenie planowania awaryjnego do SDLC zmniejsza ogólne koszty planowania awaryjnego, zwiększa możliwości awaryjne i zmniejsza wpływ na operacje systemowe, gdy plan awaryjny jest wdrażany.

7. Jaki pierwszy krok trzeba zrobić przed napisaniem ISCP?

Pierwszym krokiem w procesie planowania awaryjnego jest opracowanie deklaracji dotyczącej polityki planowania awaryjnego wspieranej przez kierownictwo wyższego szczebla (zazwyczaj dyrektora). Polityka powinna określać ogólne cele organizacji na wypadek awarii oraz powinna określać ramy organizacyjne i obowiązki planowania awaryjnego systemu informatycznego. Deklaracja polityki powinna również dotyczyć ról i obowiązków. Polityka powinna być wspierana procedurami obejmującymi wymagania szkoleniowe, częstotliwość tworzenia kopii zapasowych, składowania danych poza miejscem przetwarzania, planowanie ćwiczeń, testowanie i utrzymanie.

8. Jak można ustalić, które rozwiązania awaryjne powinno zostać wdrożone, aby zapewnić dostępność moich systemów informatycznych?

Koordynator ISCP może wykorzystać wyniki BIA do ustalenia wymagań i priorytetów planowania awaryjnego. Wyniki BIA powinny być odpowiednio uwzględnione w analizie i opracowywaniu strategii dla COOP, BCP i DRP organizacji. BIA należy wykonać podczas fazy inicjacji SDLC. W miarę ewolucji systemu i zmian komponentów, BIA może wymagać ponownego przeprowadzenia podczas fazy rozwoju / przejęcia SDLC.

BIA, która jest drugim krokiem w procesie planowania awaryjnego systemu informatycznego, ma kluczowe znaczenie dla określenia, jakie strategie odzyskiwania należy wdrożyć, aby zapewnić dostępność. BIA umożliwia Koordynatorowi ISCP pełne scharakteryzowanie komponentów systemu, obsługiwanych procesów biznesowych

i współzależności. BIA należy opracować z udziałem wszystkich powiązanych właścicieli systemów, użytkowników końcowych i partnerów systemu. Następnie można określić możliwy wpływ na organizację, związany z niedostępnością systemu informatycznego, co prowadzi do określenia RTO, średniego dopuszczalnego czasu przestoju (MTD) i sekwencji odzyskiwania elementów systemu informatycznego. Tak więc priorytety odzyskiwania będą stanowić podstawę do opracowania odpowiednich rozwiązań awaryjnych.

9. Jaki rodzaj alternatywnego miejsca przetwarzania powinienem wybrać jako strategię odzyskiwania?

Rodzaj alternatywnego miejsca powinien zostać określony przez BIA z uwzględnieniem poziomu wpływu NSC 199. Wybór alternatywnego miejsca przetwarzania musi być opłacalny i odpowiadać potrzebom systemów informatycznych organizacji. Tak więc, jeśli system wymaga prawie 100 procent dostępności, to miejsce lustrzane lub gorące może być właściwym wyborem. Jeśli jednak można pozwolić na kilka dni przestoju systemu, lepszym rozwiązaniem może być miejsce zimne.

10. Kogo i kiedy należy powiadomić w przypadku zdarzenia?

Procedury powiadamiania muszą być określone w ISCP. Koordynator ISCP powinien określić, kogo należy powiadomić, jeśli nastąpi zakłócenie systemu informatycznego i w jakiej kolejności należy się z nim skontaktować. Powiadomienia zazwyczaj obejmują właścicieli systemu, użytkowników i punkty kontaktowe. Podmioty zewnętrzne, które mogą być połączone z systemem informatycznym, powinny również zostać objęte procedurami powiadamiania. Projekt drzewa połączeń pomoże w sekwencji i przypisze odpowiedzialności za wykonywanie powiadomień do odpowiednich osób.

11. Jak często należy sprawdzać mój ISCP?

Testowanie pomaga ocenić wykonalność procedur planu, określić zdolność personelu zajmującego się odzyskiem do wdrożenia planu i zidentyfikować braki w planie. Testowanie powinno odbywać się w oparciu o wymagania organizacji oraz w przypadku wprowadzenia istotnych zmian w systemie informatycznym, obsługiwanych procesach biznesowych lub ISCP. Każdy element ISCP należy najpierw przetestować indywidualnie, a następnie jako całość, aby potwierdzić dokładność procedur odzyskiwania i ogólną skuteczność. Harmonogram testów i ćwiczeń powinien być podany w deklaracji polityki ISCP.

12. Jak często powinienem aktualizować mój ISCP?

Aktualny ISCP jest niezbędny do udanych operacji odzyskiwania. Zasadniczo ISCP należy sprawdzać pod kątem dokładności i kompletności co najmniej raz w roku, a także po

istotnych zmianach dowolnego elementu ISCP, systemu, procesów biznesowych obsługiwanych przez system lub zasobów wykorzystywanych do procedur odzyskiwania. Niedociągnięcia stwierdzone podczas testowania (patrz pytanie 11) należy usunąć podczas modernizacji planu. Elementy planu podlegające częstym zmianom, takie jak listy kontaktów, powinny być częściej sprawdzane i aktualizowane. Harmonogramy konserwacji powinny być określone w oświadczeniu o polityce ISCP.

13. Z jakimi innymi działaniami należy koordynować ISCP i rozwiązania w zakresie odzyskiwania?

Oprócz zintegrowania planowania awaryjnego z SDLC, planowanie awaryjne systemu informatycznego powinno być skoordynowane z polityką bezpieczeństwa sieci. Stosowanie stosownych zabezpieczeń systemu może pomóc w ochronie przed złośliwym kodem lub atakami, które mogłyby zagrozić dostępności systemu i są ściśle skoordynowane z procedurami reagowania na incydenty. ISCP powinien być ściśle skoordynowany ze wszystkimi innymi planami gotowości na wypadek awarii związanymi z systemem informatycznym lub połączonymi systemami i procesami biznesowymi.