



**Utrzymanie ciągłości
działania dla
wybranych
scenariuszy
kryzysowych:**

blackout, konflikt zbrojny, powódź, pandemia

Robert Wojtasiak, 04-09-2025



BNP PARIBAS

Gotówka – zabezpieczenie strategiczne

*„Choć przez lata sądzono, że gotówka stopniowo odejdzie do lamusa, ostatnie doświadczenia - pandemii, wojny, napięć geopolitycznych - pokazały jednoznacznie, że gotówka to nie relikw, lecz **zabezpieczenie strategiczne**.”*

„W momentach kryzysu to właśnie posiadanie gotówki i dostęp do niej staje się naturalną potrzebą - ludzie wypłacają gotówkę, by mieć kontrolę nad podstawowymi transakcjami, niezależnie od sieci czy pośredników technologicznych.”

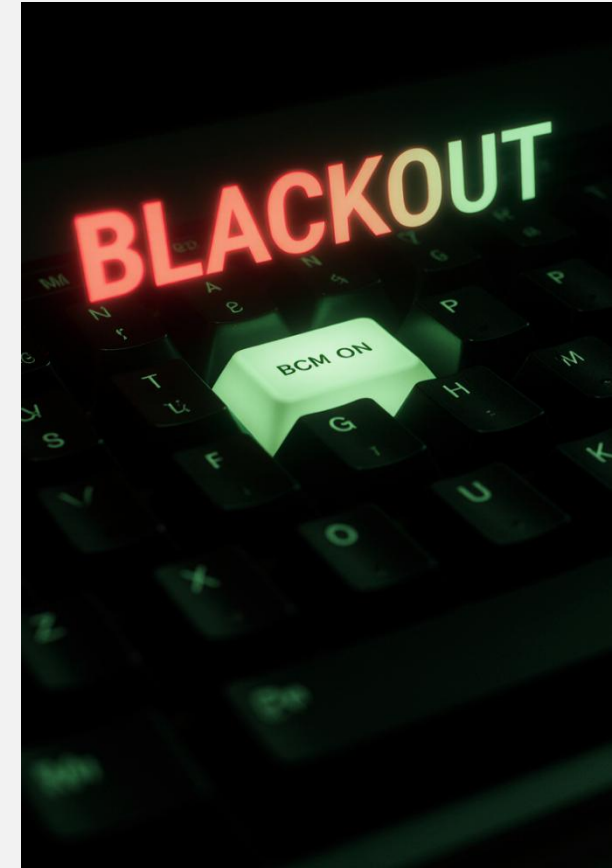
– Artur Soboń, członek zarządu Narodowego Banku Polskiego w wywiadzie dla Miesięcznika Finansowego BANK



BCP w odpowiedzi na ekstremalne scenariusze kryzysowe – blackout

(ang. Business Continuity Planning) – planowanie ciągłości działania

- Wyposażenie budynków w UPS'y oraz **systemy awaryjnego zasilania** energią elektryczną (agregaty prądotwórcze) z możliwością uzupełnienia paliwa podczas pracy agregatu. Pozwala to na zabezpieczanie systemów i aplikacji krytycznych przed awariami, umożliwiając ich ciągłą pracę.
- Przygotowanie dla budynków **planów wyłączenia** związanych z ograniczeniem dostaw energii elektrycznej - poziomy zasilania.
- Posiadanie co najmniej dwóch **Centrów Danych** (serwerowni), które są wyposażone w systemy zasilania awaryjnego z możliwością tankowania w trybie ciągłej pracy.
- Dostawcy usług Centrów Danych powinni mieć zawarte **umowy z dostawcami paliwa** wykorzystywanego do pracy ich własnych systemów awaryjnego zasilania.
- Kolokacja infrastruktury informatycznej do Centrów Danych należących do **Krajowej Infrastruktury Krytycznej** gwarantującej ciągłe zasilanie od krajowych operatorów.
- Wykorzystanie usługi **Biura Zapasowego** na scenariusz niedostępności budynków dla pracowników, którzy obsługują procesy krytyczne i nie mogą wykonywać pracy zdalnej (m.in. obostrzenia regulacyjne, bezpieczeństwa, brak zabezpieczeń gwarantowanego zasilania i dostępu do sieci Internet). Biura Zapasowe powinny być zabezpieczone w ten sam sposób co Centra Danych (patrz wyżej).
- Wyznaczenie spośród pracowników **osób kluczowych**, które są mobilizowane do pracy w trybie awaryjnym w budynkach centrali i w zapasowych lokalizacjach biur, zabezpieczonych systemami awaryjnego zasilania.
- Wyposażenie kluczowych osób (Sztab Kryzysowy) w **telefony satelitarne** lub StarLink Mini oraz **power banki**, które pokrywają najbardziej krytyczne obszary biznesowej działalności organizacji wraz z obszarami komunikacji i IT.
- Potwierdzenie u **dostawców Internetu** (łącza dzierżawione) ich **odporności na przerwy w zasilaniu** poprzez wykorzystanie ich własnego systemu zasilania awaryjnego.
- Wyposażenie kluczowych/największych oddziałów oraz bankomatów w systemy awaryjnego zasilania i **satelitarnego dostępu do Internetu**, w celu zabezpieczenia ciągłości obsługi, w tym wypłat gotówki.



BNP PARIBAS

BCP w odpowiedzi na ekstremalne scenariusze kryzysowe – konflikt zbrojny

(ang. Business Continuity Planning) – planowanie ciągłości działania

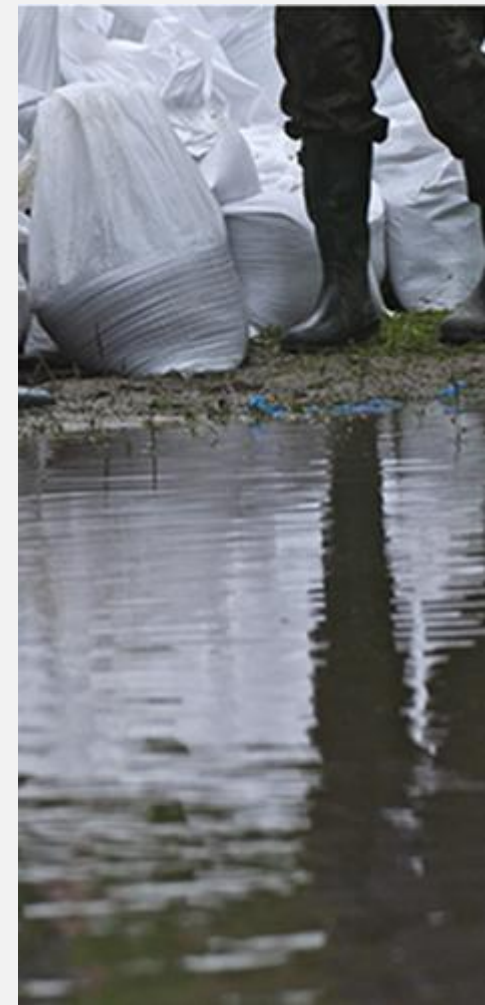
- **Przejęcie działań operacyjnych** przez biura lub oddziały zlokalizowane w różnych miastach / krajach – w ramach możliwości.
- **Ewakuacja** pracowników na tereny zabezpieczone np. wykorzystanie oddziałów, tymczasowe zakwaterowanie w pobliskich hotelach, wykorzystanie infrastruktury oddziału do pracy zdalnej oraz wykorzystanie Zapasowych Biur.
- Wykorzystanie jak we wcześniejszym scenariuszu **telefonii satelitarnej** oraz **satelitarne go dostępu do Internetu** dla zapewnienia komunikacji głosowej i Internetowej / VPN.
- **Sztab Kryzysowy** w przypadku niedostępności jego Szefa i zastępcy będzie zarządzany przez kolejne wyznaczone osoby
- Posiadanie co najmniej dwóch **Centrów Danych** w dużej odległości geograficznej.
- Stworzenie i utrzymywanie **bezpiecznej kopii najistotniejszych danych krytycznych** systemów i aplikacji przy wykorzystaniu rozwiązań chmurowych oraz wirtualizacyjnych przy wykorzystaniu odpowiedniego szyfrowania.
- Opracowanie oraz stosowanie odpowiednich **założeń architektury technicznej** mającej na celu zapewnienie spójności danych podczas odtwarzania (ang. disaster recovery) po wystąpieniu rozległych awarii IT obejmujących większą część lub całość Centrum Danych.
- **W oddziałach gotówkowych** w przypadku zagrożenia należy gotówkę przetransportować do innych centrów kasowych.
- W przypadku niemożności transportu, alternatywnie - **przeniesienie banknotów do formy niezdatnej do użytku**: jedna część banknotu - 50% zostaje zniszczona w niszczarce, kolejna część banknotu - 50% jest zabezpieczona w sejfie w oddziale w celu dalszego transportu do NBP po ustaniu zagrożenia. **Uwaga!** Dotyczy waluty krajowej. W przypadku zniszczenia obcej waluty brak rekompensaty od NBP. Stąd akumulacja rezerw walutowych wiąże się z ryzykiem.



BCP w odpowiedzi na ekstremalne scenariusze kryzysowe – powódź

(ang. Business Continuity Planning) – planowanie ciągłości działania

- W ramach działań związanych z bezpieczeństwem pracowników i klientów oraz zapewnieniem ciągłości operacyjnej należy stosować **ciągłe monitorowanie sytuacji** związanej ze zwiększonym ryzykiem wystąpienia **zagrożenia powodziowego** na obszarze Europy Środkowej, a w szczególności na południu Polski.
- Należy przygotować i uruchomić **komunikację** informując o podstawowych krokach postępowania w przypadku zagrożenia powodziowego, mających na celu zapewnienie bezpieczeństwa ludzi oraz utrzymanie ciągłości operacyjnej.
- Można zastosować m.in. **pracę zdalną**, wykorzystanie biurowych **Lokalizacji Zapasowych** na terenach wolnych od zagrożenia powodziowego.
- Powołany **Sztab Kryzysowy** pozyskuje aktualną informację w miarę możliwości bezpośrednio od pracowników z terenów zagrożonych powodzią a dotyczącą ich bezpieczeństwa oraz informację o stanie oddziałów, ich dostępności, przerwach w dostawie prądu, dostępności bankomatów, bezpieczeństwie skarbców, organizacji **dostępu do gotówki**.
- Monitorowanie sytuacji oddziałów w czasie rzeczywistym jest możliwe poprzez **wykorzystanie systemu całodobowego monitoringu wizyjnego**.
- Wykorzystanie **lokalnych patroli ochrony** umożliwia weryfikację bezpieczeństwa fizycznego oddziałów,
- Obszar komunikacji przygotowuje i publikuje odpowiednią **komunikację** zarówno wewnętrzną jak i zewnętrzną dostosowaną do bieżącej sytuacji.
- **Biuro bezpieczeństwa CERT** przestrzega przed fałszywymi informacjami tzw. fake news, oraz przypomina o tym, że należy polegać tylko na oficjalnych źródłach wiadomości.
- W ramach **Związku Banków Polskich**, który pozostaje w komunikacji z Urzędem Komisji Nadzoru Finansowego otrzymujemy informacje o ewentualnym negatywnym wpływie sytuacji powodziowej na stabilność sektora finansowego, w tym o możliwości wystąpienia przejściowych i lokalnych problemów z **dostępnością do gotówki** na obszarach dotkniętych powodzią.



BNP PARIBAS

BCP w odpowiedzi na ekstremalne scenariusze kryzysowe – pandemia

(ang. Business Continuity Planning) – planowanie ciągłości działania

- Powołanie **Sztabu Kryzysowego** w celu monitorowania bieżącej sytuacji i podejmowania odpowiednich decyzji
- Śledzenie na bieżąco **komunikatów rządowych** odnośnie statusu/zaleceń w sprawie rozprzestrzeniania się pandemii.
- Przygotowanie **komunikacji dla pracowników** na podstawie bieżących informacji - komunikacja powinna zawierać oficjalne informacje ze stron instytucji rządowych aby nie wywołać paniki wśród pracowników, powinna być aktualizowana cyklicznie zgodnie z pojawiającymi się informacjami na temat rozwoju sytuacji.
- **Wstrzymanie podróży/delegacji** w tym zagranicznych oraz nieprzyjmowanie gości również z zagranicy o ile nie jest to konieczne.
- Wprowadzenie podziału zespołów na tych pracujących zdalnie i w biurze – **praca rotacyjna** w celu zminimalizowania zarażenia całych zespołów;
- Stosowanie **kwarantanny domowej** dla pracowników zarażonych (wyniki testów, podwyższona temperatura, podróże osób w obszarach wysokiego ryzyka).
- **Magazynowanie** odpowiedniej liczby masek oraz w przypadku wystąpienia pandemii dodatkowy **zakup i dystrybucja masek** dla pracowników w biurach i oddziałach.
- Stosowanie **mydła i płynów antybakteryjnych** przez pracowników. Wprowadzenie systemu automatycznego badania temperatury przy wejściu do budynku (za zgodą pracowników).
- **Zabezpieczenie budynków w tym oddziałów i recepcji** w płyty plexi, ozonowanie pomieszczeń, wprowadzenie zasad poruszania się i organizacji spotkań w budynkach.
- **Odwołanie imprez zbiorowych** - duże wewnętrzne i zewnętrzne wydarzenia biznesowe.
- Weryfikacja pod względem prawnym możliwości pracy zdalnej **Zarządu i Rady Nadzorczej**.
- Zwiększenie **dystrybucji gotówki** do bankomatów i wprowadzenie **limitów wypłat gotówkowych**.



DZIĘKUJĘ ZA UWAGĘ
!