

Blok 2

**Sektor bankowy w obliczu kryzysu
wywołanego wojną w Ukrainie**

Ciągłość działania banków

**dr Jarosław Biegański
FinCERT.pl – Bankowe Centrum
Cyberbezpieczeństwa ZBP**

Warszawa, 1 czerwca 2022 r.



„Nigdy w swoich planach nie zakładaliśmy bombardowania”

**Mariusz Kaczmarek
wiceprezes PrivatBanku**



Przykłady wyzwań dla sektora finansowego

- Dostępność gotówki
- Dostępność usług elektronicznych
- Sprawne zasilanie awaryjne
- Kaskadowe alarmy bombowe
- Zdolność dostawców do świadczenia usług
- Wzajemna pomoc i wymiana informacji

Źródła:

<https://strefabiznesu.pl/gotowki-w-bankomatach-nie-zabraknie-moga-pojawic-sie-przejsciowe-klopoty-co-z-pieniedzmi-w-oddzialach-bankow/ar/c3-16073197>

https://media-exp1.licdn.com/dms/image/C4E22AQHWvUf2h_ZKgQ/feedshare-shrink_1280/0/1651233103944?e=1654732800&v=beta&t=yliGAbvYtYQtHJr5JdN86x054zg_L2_c4FsdUZBI5a1A

<https://silesia24.pl/wiadomosci/szczegoly/poczta-polska-przekazala-ukrainie-opancerzoe-bankowozy-do-przewozu-gotowki-35109>





Ludzie a ciągłość działania

„Mieliśmy przetrwać
dwa tygodnie”
wywiad miesiąca
Miesięcznika
Finansowego BANK
- kwiecień 2022

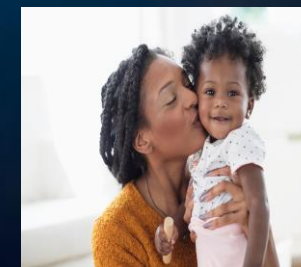
Ochotnicy oraz powszechna mobilizacja



Fizyczne bezpieczeństwo pracowników



Stres związany z osobistym ryzykiem
oraz troska o zagrożenie fizyczne
egzystencji najbliższych



Niechęć pracowników do ewakuacji



„Dochodzi jeden
czynnik, którego
nigdy nikt nie brał
pod uwagę”
Mariusz
Kaczmarek,
wiceprezes
PrivatBanku



Rekomendacje Zarządu ZBP

Wydane jako samoregulacja - odpowiedź sektora bankowego na zidentyfikowane rodzaje ryzyka operacyjnego.

Ich stosowanie zwiększa odporność na zagrożenia dla bezpieczeństwa i ciągłości działania oraz wzmacnia skuteczną reakcję na przestępstwa.

Zarząd ZBP między innymi przyjął rekomendacje dotyczące:

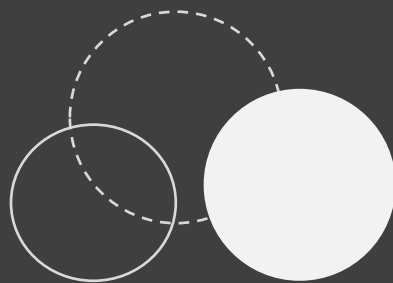
- *przeciwdziałania niedostępności bankowych serwisów internetowych w wyniku ataków DoS/DDoS – 8 lutego 2022 r.*
- *zachowania ciągłości działania banków w obliczu międzynarodowego konfliktu zbrojnego lub wojny hybrydowej – 10 marca 2022 r.*
- *dotyczące kaskadowych gróźb ataków na placówki bankowe – 29 grudnia 2020 r.*





Rozpoznane rodzaje ryzyka

Celem Rekomendacji jest ograniczenie możliwości wystąpienia zidentyfikowanych rodzajów ryzyka lub minimalizacji skutków ich materializacji w postaci negatywnego wpływu na ciągłość działania i dostępność usług i produktów bankowych na terenie Polski



Brak realizacji lub zakłócenia w realizacji operacji bankowych oraz obsługi pozostałych krytycznych obszarów działalności banku

Niezachowanie właściwej komunikacji z klientami oraz niewłaściwa komunikacja wewnątrz organizacji (niedopuszczenie do paniki – wywołania efektu „kuli śnieżnej”)

Utrata kontroli nad treścią komunikatów wychodzących z banków za pośrednictwem mediów społecznościowych:

Długotrwała niedostępność usług lub produktów bankowych w kanałach zdalnych

Brak realizacji lub zakłócenia w realizacji zadań placówek terenowych sieci własnej lub franczyzy

Brak realizacji lub zakłócenia w realizacji zarządzania gotówką

Brak realizacji lub zakłócenia w realizacji Contact Center - rozmowy przychodzące i wychodzące.

Brak dostępności kluczowej kadry menedżerskiej banku lub pracowników realizujących krytyczne procesy lub brak możliwości wykonywania zadań przez nich

Wprowadzenie stref ograniczonego ruchu osobowego

Wzmocniony ruch transakcji elektronicznych

Obniżenie poziomu zabezpieczeń w dostępie do bankowych systemów IT

Możliwość wystąpienia incydentów wymierzonych w bezpieczeństwo banków lub ich klientów

Utrata standardowych kanałów komunikacji lub ich znacząca destabilizacja

Ziszczenie się powyższych rodzajów ryzyka w całym sektorze bankowym

Utrata zasilania elektroenergetycznego (Blackout)

Możliwość utraty danych

Niedostępność usług publicznej chmury obliczeniowej wspierającej procesy bankowe, kluczowe z punktu widzenia ich dostępności

Niedostępność bankowych usług outsourcingowych z obszaru IT, kluczowych z punktu widzenia ich dostępności

Jednoczesna niedostępność lub utrata centrów danych (podstawowego i zapasowych)



Dziękujemy za uwagę

FinCERT.pl – Bankowe Centrum
Cyberbezpieczeństwa ZBP

kontakt: bcc@zbp.pl
alert@fincert.pl

Lista komunikatów i ostrzeżeń FinCERT.pl – BCC ZBP

<https://zbp.pl/Dla-Bankow/Cyberbezpieczenstwo/Listakomunikatow-i-ostrzezen-FinCERT-pl-%E2%80%93-BCC-ZBP>