Zdążyć przed kryzysem - wersja BAZOWA

Cel → przygotować komunikację na rok 2026, w którym kryzysy najczęściej startują online, szybko eskalują i testują odporność operacyjną. Jeśli zrobisz tylko to, zyskujesz realną odporność na kryzysy online, dezinformację i mikrokryzysy.

Fundament: kto decyduje i gdzie jest prawda

1

Jedno miejsce prawdy: stały link/landing „Komunikaty" (WWW/newsroom) + zasada: zawsze tam odsyłamy.
Tryb kryzysowy: kto podejmuje decyzje i kto publikuje (zastępstwa + kontakt po godzinach).
Lista kontaktów krytycznych: zarząd, PR/Comms, legal, IT/security, HR, operacje, partnerzy zew + aktualizacja co kwartał.

Internet-first: wykryj zanim wybuchnie

2

Monitoring + alerty: social/media/fora/komentarze (choćby minimum manualne, ale codziennie).
Radar sygnałów: 10 rzeczy, które mają alarmować (np. „oskarżenia", „zagrożenie bezpieczeństwa", „wideo/screen", „trend w grupach").
Kanał zgłoszeń wewnętrznych: pracownicy/BOK/sprzedaż/obsługa wiedzą, gdzie zgłosić „co mówi rynek".

Dezinformacja i fake news: gotowce i procedura

3

Top 10 prawdopodobnych narracji (plotek/zarzutów) — spisane na 1 stronie.
Do każdej narracji: odpowiedź w 2–3 zdaniach + źródło/dowód + FAQ (minimum).
Mini-procedura debunkingu: monitoring → weryfikacja → reakcja → śledzenie (kto, gdzie, kiedy).

Pierwsze 60 minut: jeden szablon dla całej organizacji

4

Stosuj model 4W: Co wiemy / Czego nie wiemy / Co wdrażamy / Kiedy wrócimy.
Zasada: pierwszy komunikat w 30–60 minut (nawet jeśli to „sprawdzamy i wrócimy o...").
Gotowiec „pierwszej odpowiedzi" dla 4 scenariuszy: (1) awaria/usługa, (2) zarzut reputacyjny, (3) kryzys pracowniczy, (4) incydent cyber.

Mikrokryzysy: zarządzaj codziennością, bo ona buduje (lub psuje) reputację

5

3 proste KPI: czas reakcji / jakość odpowiedzi / deeskalacja.
15-min przegląd raz w tygodniu: „co zapłonęło" + 3 wnioski + poprawki do gotowców/Q&A.

Cyber i phishing: minimum, które ratuje reputację

6

MFA (uwierzytelnianie wieloskładnikowe) na: poczcie/SSO, zdalnym dostępie, narzędziach publikacji, kontach administracyjnych.
Phishing drill raz na kwartał (15 min) + zasada: nie klikamy — weryfikujemy innym kanałem.
Instrukcja „co robić po kliknięciu" + kultura „zero wstydu" (zgłaszamy natychmiast).

Jedno ćwiczenie, które spina całość

7

1 symulacja/rok: fake news + eskalacja w social + pytania mediów + wątek operacyjny.
Po ćwiczeniu: 5 poprawek + właściciele + termin wdrożenia (do 14 dni).

Test gotowości (60 sekund)
Jeśli masz: (1) jedno miejsce prawdy, (2) monitoring + radar, (3) Top 10 narracji z gotowcami, (4) szablon 60 min., (5) MFA + phishing — jesteś w bezpiecznym minimum na 2026.