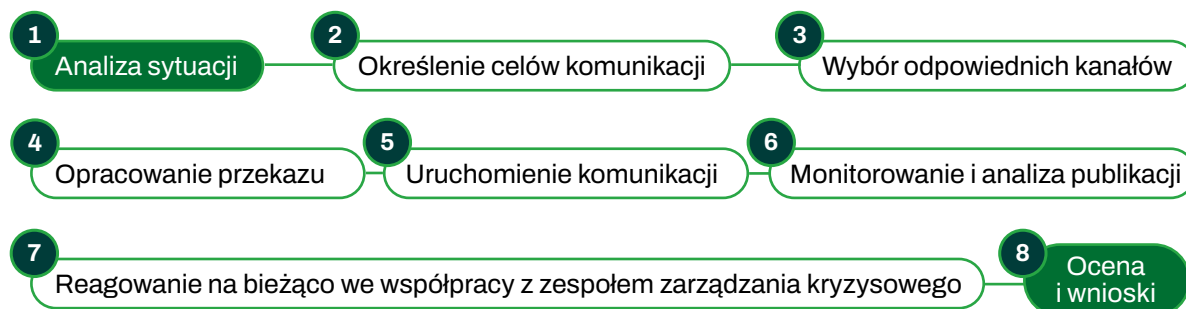


Komunikacja kryzysowa w cyberbezpieczeństwie

Zasady skutecznej komunikacji podczas incydentu



Komunikacja kryzysowa krok po kroku



Kogo, jak i gdzie informować?



Kogo informować?

Tych, którzy odczują skutki.

- **klienci** / użytkownicy usług
- **pracownicy**
- **partnerzy i dostawcy**
- **media / opinia publiczna**



Co mówić?

To, co jest dla nich praktycznie ważne.

- **klienci** „czy jestem zagrożony i co mam zrobić?”
- **pracownicy** „jak odpowiadać i jakie są zasady?”
- **partnerzy** „czy to wpływa na współpracę?”
- **media** „co się stało i jaka jest skala?”



Gdzie mówić?

Tam, gdzie są interesariusze i gdzie oczekują informacji

- **Klienci:** strona internetowa, komunikat na stronie głównej lub w panelu klienta, e-mail, SMS, infolinia, aplikacja mobilna (powiadomienia push), media społecznościowe, sekcja FAQ.
- **Pracownicy:** intranet, e-mail, komunikatory firmowe, spotkania, webinary wewnętrzne, komunikaty od przełożonych, newsletter wewnętrzny.
- **Partnerzy biznesowi:** bezpośredni kontakt, opiekunowie klientów, dedykowane wiadomości e-mail, portale partnerskie, webinary lub spotkania informacyjne.
- **Media:** oficjalne oświadczenie, komunikat prasowy, konferencja prasowa, briefing dla dziennikarzy, sekcja prasowa na stronie internetowej.
- **Organy nadzoru i instytucje publiczne:** dedykowane kanały zgłoszeniowe, oficjalna korespondencja, systemy teleinformatyczne właściwych organów.
- **Inwestorzy i akcjonariusze:** raporty bieżące, komunikaty korporacyjne, spotkania informacyjne, relacje inwestorskie.



Zawsze warto korzystać z kilku kanałów jednocześnie, aby zwiększyć szansę dotarcia do wszystkich grup odbiorców i zapewnić spójność przekazywanych informacji.



Co powinien zawierać komunikat?

Dobry komunikat odpowiada na podstawowe pytania:



- Co się wydarzyło?
- Kogo dotyczy incydent?
- Jaki jest wpływ na odbiorców?
- Jakie działania prowadzi organizacja?
- Co powinien zrobić odbiorca?
- Kiedy pojawią się kolejne informacje?



Jak komunikować incydent?

Dobre praktyki



- **Komunikuj** się szybko
- **Informuj** zgodnie z aktualnym stanem wiedzy
- **Bądź transparentny**
- **Pisz prostym** i zrozumiałym językiem
- **Aktualizuj komunikaty** wraz z rozwojem sytuacji
- **Zachowaj spójność przekazu** we wszystkich kanałach
- **Przekazuj** praktyczne wskazówki odbiorcom

Najczęstsze błędy



- **Opóźnianie** pierwszego komunikatu
- **Czekanie** na pełne ustalenie wszystkich okoliczności
- **Spekulacje** i niepotwierdzone informacje
- **Nadmiernie** techniczny język
- **Brak** kolejnych aktualizacji
- **Niespójne** komunikaty w różnych kanałach
- **Składanie deklaracji**, których nie można dotrzymać



Należy pamiętać, że każdy incydent powinien zostać wykorzystany jako źródło doświadczeń, które pozwolą zwiększyć gotowość organizacji do reagowania na kolejne sytuacje kryzysowe.



Dlaczego komunikacja ma znaczenie?

Komunikacja jest integralnym elementem reagowania na incydenty cyberbezpieczeństwa. Jej celem jest ograniczenie skutków incydentu, wsparcie odbiorców oraz realizacja obowiązków wynikających z przepisów prawa. Brak komunikacji to brak kontroli – szybki, rzetelny komunikat ogranicza skalę kryzysu.

Skuteczna komunikacja:



- pomaga ograniczyć skutki incydentu,
- umożliwia użytkownikom podjęcie działań ochronnych,
- przeciwdziała dezinformacji i spekulacjom,
- pozwala zachować kontrolę nad narracją,
- buduje zaufanie do organizacji,
- ogranicza ryzyko reputacyjne i biznesowe,
- wspiera realizację obowiązków prawnych.



Kiedy komunikacja jest obowiązkowa?



Podmiot kluczowy lub ważny ma obowiązek* poinformować użytkowników m.in. o:

- poważnym cyberzagrożeniu mogącym wpływać na świadczone usługi,
- incydencie poważnym wpływającym na świadczenie usług,
- środkach, które użytkownicy mogą podjąć w celu ograniczenia skutków zagrożenia.

*Podstawa prawna: art. 11 ust. 2a–2b ustawy o krajowym systemie cyberbezpieczeństwa



Brak wymaganej komunikacji może skutkować wydaniem przez właściwy organ decyzji administracyjnej nakazującej poinformowanie odbiorców usług (art. 53 ustawy o KSC). Przejrzysta i rzetelna komunikacja w obszarze incydentów cyberbezpieczeństwa świadczy o odpowiedzialności i dojrzałości organizacji. Transparenność wobec klientów i partnerów biznesowych buduje wizerunek firmy, dlatego informowanie o incydentach zalecamy każdej instytucji dotkniętej incydem – nie tylko tym, które mają taki obowiązek.