Katarzyna Grabowska
NASK

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

Iwona Prószyńska
NASK

Rozmowa z Iwoną Prószyńską, Kierownik Zespołu ds. Strategicznej Komunikacji Cyberbezpieczeństwa, NASK.

KG: Jak zaczęła się Twoja przygoda z cyberbezpieczeństwem?

IP: Najpierw były regulacje w obszarze cyberbezpieczeństwa – te krajowe i międzynarodowe. Pochłaniały mnie aspekty prawne, to było pokłosie moich zainteresowań jeszcze z okresu studiów. Zobaczyłam jednak, że cyberbezpieczeństwo, to też część techniczna –trudniejsza, ale nagle z mojej perspektywy bardzo ciekawa. Tak zaczęłam pracę w CERT Polska i od tej chwili potoczyło się już bardzo szybko. Poszłam na studia z tego obszaru i skupiłam się na tym, co wychodzi mi najlepiej – mówieniu o rzeczach ważnych (ale też trudnych) w sposób przystępny. Istotnym elementem mojej codziennej pracy jest też wsparcie firm i instytucji mierzących się z incydentami – komunikacja kryzysowa jest wpisana w cyberbezpieczeństwo. Dziś już wiem, że to obszar, w którym chcę się dalej rozwijać. Praca dla CSIRT-u poziomu krajowego to dużo wyzwań, ale też olbrzymia satysfakcja.

KG: Twoim zdaniem komunikacja kryzysowa w cyberbezpieczeństwie różni się od tej w innych obszarach?

IP: Zasady są praktycznie takie same, trzeba natomiast pamiętać, że komunikowanie incydentów wymaga pewnej wiedzy z obszaru cyberbezpieczeństwa. Żeby jasno wyjaśnić co się wydarzyło, trzeba to najpierw zrozumieć, skomplikowany język techniczny przełożyć na komunikat, który dotrze do każdego. Specyfika incydentów np. dużych wycieków danych, które

są pokłosiem ataków ransomware, sprawia też, że odbiorców komunikacji jest bardzo wielu. Nawet kilka milionów osób może w jednym czasie otrzymać informację, że ich wrażliwe dane zostały upublicznione w sieci. To prawdziwy kryzys wizerunkowy.

KG: Jaki był najtrudniejszy incydent, z którym miałaś do czynienia, i jak udało się go opanować komunikacyjnie?

IP: Każdy jest wyzwaniem, bo w grę wchodzi stres, ryzyko utraty reputacji, niepokój klientów. Rozumiem te emocje, ale moja przewaga jest taka, że mogę podejść do tego "na chłodno" - ocenić sytuację, doradzić jak pokierować komunikacją.

KG: Czy zauważasz zmianę podejścia do komunikowania incydentów w organizacjach?

IP: Myślę, że pierwszą istotną zmianą jest to, że instytucje, które mierzą się z incydentem przychodzą po wsparcie, że szukają rad i wskazówek jak informować. Wcześniej dość często stosowano taktykę "zamiatania pod dywan", ale to była dość krótkowzroczna strategia, bo jak klienci dowiadywali się np. z mediów, że ich dane wyciekły, to straty wizerunkowe były już nie do nadrobienia. Dużo mówimy też o profilaktyce – wiele firm ma dzięki temu gotowe plany działania na wypadek sytuacji kryzysowej. Znają też swoich klientów - wiedzą do kogo i jak mają mówić, a to bardzo ważne, szczególnie w pierwszej fazie kryzysu. I to także pewna nowość względem tego, jaka była świadomość zaledwie kilka lat wstecz.

KG: Jakie są najważniejsze działania, które powinna podjąć organizacja w przypadku wystąpienia incydentu i jakie wnioski może

CyberTalk, czyli cyberbezpieczeństwo oczami kobiet

wyciągnąć by ulepszać swoje procedury?

IP: To bardzo dobre pytanie i dotyka ważnej kwestii, bo właśnie trzeba zacząć od tego, żeby mieć procedury. Plany działania na wypadek kryzysu to dziś must have. Możemy tam zapisać np. kto tworzy zespół obsługujący incydent.
Jeśli myślimy o kryzysach, które mają potencjał medialny, to w ich wypadku równolegle do działań "technicznych" powinny iść te komunikacyjne. Zespół obsługujący takie zdarzenie powinny tworzyć osoby techniczne, IOD, ale też pracownicy odpowiedzialni za komunikację.

KG: Jakie są najczęściej popełniane błędy w komunikacji kryzysowej podczas incydentów cyberbezpieczeństwa?

IP: Zacznijmy od tego jak to ma modelowo wyglądać. Komunikacja incydentu powinna być prowadzona jasno, szczerze, na czas, ze zrozumieniem emocji klientów. To kluczowe elementy dobrze poprowadzonych działań informacyjnych, ale też te które zawodzą najczęściej. Wciąż zdarza się, że komunikaty pojawiają się z opóźnieniem, zamiast o ataku mówią o "awarii", ich język jest albo bardzo techniczny albo bazuje na zapisach z regulacji prawnych z tego obszaru, więc bez pomocy prawnika trudno go zrozumieć. To błędy, których można i trzeba unikać.

KG: Jakie kompetencje powinna rozwijać osoba planująca podążać podobną ścieżką kariery do Twojej?

IP: Tak jak wcześniej wspomniałam - potrzebny jest pewien zasób wiedzy technicznej, ale to można uzupełnić np. podczas studiów podyplomowych. Z umiejętności bardziej miękkich potrzeba empatii, która pomaga

budować zaufanie, a ono jest kluczowe. Przydaje się lekkie pióro, otwartość, elastyczność. Ale do obszaru komunikacji incydentów można też podejść z drugiej strony. Wiedza techniczna i chęć rozwijania kompetencji miękkich, to równie dobra i skuteczna droga. Niezależnie od obranej ścieżki przyda się determinacja i świadomość, że to praca z misją. Owszem wyzwań jest dużo, ale na koniec dnia można z dumą pomyśleć, że dzięki naszym działaniom rośnie cyberbezpieczeństwo bardzo wielu osób.

KG: Dziękuję za rozmowę. Rozwiązania techniczne i komunikacja kryzysowa odgrywają kluczową rolę w skutecznym reagowaniu na incydenty cyberbezpieczeństwa. Komunikacja w tym zakresie to nie tylko sztuka reagowania, ale też empatia, jasność przekazu i dobre przygotowanie.

IP: Dziękuję!