Warszawa, 09.06.2021 r.

Dzień z życia IOD-y

- fabularyzowany opis obsługi incydentu - wszelkie podobieństwa do osób/klientów/niepotrzebne skreślić przypadkowe ;-)

I znowu mamy poniedziałek. W dodatku poniedziałek po długim weekendzie. Bajka…. Już z samego rana wszystkim IOD towarzyszy myśl, czy będzie to bajka, w której będzie nam towarzyszyć armia dobrych wróżek oraz krasnoludków (wiadomo – im większy zespół, tym więcej rąk do pracy), czy raczej zjawi się zła królowa, chcąca wcisnąć nam zatrute jabłko. Najważniejsze jednak, aby w polu widzenia nie pojawił się on. On, czyli incydent.

Nikt nie lubi incydentów i administratorzy danych wspomagani przez IOD robią wszystko, aby do nich nie dopuścić. Niestety, lwia część incydentów wynika z błędu człowieka, a przed tym ciężko się ustrzec. Nawet jeśli pracownicy są przeszkoleni oraz świadomi zagrożeń, zazwyczaj pracują pod presją czasu, a ta jest bardzo incydentogenna. Tak czy inaczej, zawsze lepszy incydent w poniedziałek z rana niż w piątek po południu… Nieciekawa sytuacja jest też wtedy, gdy incydenty zdarzają się w okresach świątecznych lub urlopowych. Wówczas dodatkowo często trzeba mierzyć się z sytuacją, w której np. pracownik posiadający wiedzę na temat zdarzenia jest na urlopie. Ale odrzućmy od siebie te złe myśli i zajmijmy się czekającymi na nas zadaniami. Mam do analizy kilka umów i procedur, klauzule do dostosowania, rozgrzebany raport do dokończenia, szkolenie online do przeprowadzenia oraz wszystko to, co zawita po drodze, czyli najczęściej telefony, pilne sprawy wpadkowe i właśnie incydenty. Tych ostatnich nie darzymy sympatią, gdyż nie dość, że mogą być ryzykowne dla administratora, to jeszcze patrząc na sprawę z perspektywy pracowniczej, burzą plan pracy i skutkują opóźnieniami w wykonywaniu innych zadań. Jest to szczególnie niekomfortowe, gdy obiecaliśmy klientowi np. zaopiniowanie długaśnej umowy dzisiaj do końca dnia, a nagle wskakuje incydent i w jednej chwili burzy ten ambitny plan.

No ale do dzieła. Dzień chwilowo mija spokojnie i mimo dużej ilości zadań, praca dobrze idzie. W jakiej kolejności są wykonywane zadania? Ja robię je zgodnie z chronologiczną kolejnością wpływu a zatem najpierw to, co jako pierwsze wpadło na skrzynkę. Oczywiście od tej zasady są wyjątki i dotyczą one m.in. konsultacji telefonicznych, które czasami trwają 5 minut a czasami pół godziny lub nawet godzinę. Zależy jak bardzo skomplikowana jest omawiana kwestia. Fajnie, jeśli temat jest już znany i można szybko pomóc. Jeżeli jednak zagadnienie wymaga analizy, wtedy należy poświęcić mu więcej

czasu. Wyjątek stanowi również sytuacja, która jest dosyć istotna,
ale nie jest czasochłonna i można ją wykonać między innymi zadaniami, np. ustalanie terminów call'i czy szkoleń prowadzonych w formie webinarów lub odpowiadanie na maile niewymagające dużego zaangażowania. Zdarza się, że ze względu na ilość spraw pojawiających się na bieżąco ciężko wygospodarować czas na pracę projektową.

Po kilku telefonach i odesłaniu przeanalizowanych umów przychodzi pora na krótką przerwę obiadową. Po niej przeprowadzenie szkolenia i planuję zająć się rozpoczętym raportem. I w tym momencie mamy klasyk – gdy tylko siadam do raportu, otrzymuję telefon w sprawie podejrzenia wystąpienia incydentu. Przesłanie dokumentacji do nieodpowiedniego klienta, czyli najczęstszy przypadek naruszenia. Dodatkowo, pracownik posiadający wiedzę na temat zdarzenia od jutra będzie niedostępny przez kilka dni, więc wszystkie informacje trzeba zebrać dzisiaj. Jeśli zdarza się tak, że najpierw otrzymuję telefon w sprawie potencjalnego incydentu, rozmawiam o zdarzeniu, a później przesyłam mailem zestaw pytań dotyczących zdarzenia, aby doprecyzować niezbędne kwestie. Jeśli o incydencie jestem zawiadamiana mailem - i tak dzwonię, gdyż pewne rzeczy łatwiej i szybciej jest omówić ustnie. Pytania przesyłam zawsze na skrzynkę pocztową, aby pracownik administratora miał je przed oczami i mógł precyzyjnie opracować odpowiedzi. Zazwyczaj odpowiedź otrzymuję następnego dnia. W końcu na zgłoszenie naruszenia są 72 h od jego stwierdzenia, jednak w sytuacji, w której osoba mogąca udzielić informacji będzie nieobecna, wszystko muszę zebrać dzisiaj. Pisanie raportu chyba trzeba będzie przełożyć.

Na szczęście w przeciągu godziny otrzymuje informację zwrotną na moje pytania. W umowie był zawarty nr PESEL a zatem mamy do czynienia z naruszeniem i trzeba będzie przesłać zgłoszenie do UODO oraz powiadomić osobę, której dane dotyczą, czyli w tym przypadku przekazać klientowi, że umowa z jego danymi osobowymi przez pomyłkę (wspominałam już o pracy pod presją czasu?) została przesłana do innego klienta. W mailu, który otrzymałam niby jest wszystko to, o co prosiłam, ale brakuje mi pewnych szczegółów, które muszę znać, aby odpowiednio przygotować zgłoszenie do UODO, a zatem dzwonię, aby dopytać. Odpowiedź mam otrzymać mailem w ciągu 15 minut i rzeczywiście tak się dzieje. Teraz można przystąpić do dalszych działań. Najpierw trzeba zaradzić sytuacji. Jeśli nie zrobiono tego wcześniej, proszę, aby pracownik administratora, u którego doszło do naruszenia powiadomił o zdarzeniu klienta, do którego przesłano przez pomyłkę umowę oraz klienta, którego umowę błędnie przesłano. Z klientem, który otrzymał umowę zawierającą dane osobowe należy ustalić sposób jej zwrotu (np. odebranie umowy przez kuriera) a także poprosić go, aby nie otwierał przesyłki (o ile nie została już otwarta) oraz nie kopiował danych a także nie udostępniał ich innym osobom. Oprócz tego zalecam jak najszybsze powiadomienie o incydencie głównego poszkodowanego, czyli osoby, której dane dotyczą. Z mojego doświadczenia wynika, że najlepiej, gdy pierwszy kontakt jest telefoniczny (jeśli dysponujemy numerem telefonu). Jest to przede wszystkim szybki sposób kontaktu, który pozwala na dokładne wyjaśnienie w czasie rozmowy co zaszło, z czym to się wiąże, co zostało już zrobione oraz jakie będą kolejne kroki. Dopiero po tym

przesyłany jest mail z oficjalną informacją, przy czym osoby są uprzedzane o tym, że otrzymają wiadomość na skrzynkę pocztową i nie są już zaskoczone. Przekazanie informacji w sposób pozwalający na wykazanie, że zostało to wykonane jest niezbędne ze względu na zasadę rozliczalności, a mail jest dobrym narzędziem. Oczywiście, jeśli naruszenie dotyczyłoby dużej grupy osób dzwonienie byłoby raczej niemożliwe. Samodzielnie przygotowuję treść informacji, która będzie przesłana do osoby, której dane zostały naruszone (zgodnie z wymogami wskazanymi w art. 34 RODO) oraz do osoby, do której trafiły dane i proszę pracowników administratora o przesłanie ich jeszcze dzisiaj. Sama przystępuję do przygotowania formularza zgłoszenia naruszenia do UODO. Staram się opisać wszystko tak prosto i klarownie jak się da. Tam po drugiej stronie siedzą ludzie, którzy to czytają i muszą wiedzieć co dokładnie się wydarzyło. Jeśli jakieś kwestie wskazane w zgłoszeniu pozostaną niejasne, UODO prześle pismo, w którym poprosi o doprecyzowanie informacji, dlatego najlepiej wskazać wszystko od razu. Uzupełniony formularz przesyłam do UODO za pomocą profilu zaufanego, posiadając do takiej czynności pełnomocnictwo od administratora danych. Ważną kwestią jest to, aby posiadać pełnomocnictwo do zgłaszania naruszeń. Głupio byłoby, gdyby okazało się, że nikt nie posiada odpowiedniego pełnomocnictwa a osoba, która zgodnie z zasadami reprezentacji podmiotu powinna przesłać zgłoszenie jest na urlopie lub leży chora w szpitalu. Takie dodatkowe atrakcje powodują tylko skoki ciśnienia i należy się ich wystrzegać dbając zawczasu o nadanie pełnomocnictwa.

Dobra, zgłoszenie przesłane do UODO. To teraz pozostaje tylko uzupełnić wewnętrzny rejestr naruszeń i… dzień się kończy. Miejmy nadzieję, że dzisiejsze naruszenie wyczerpało limit na ten tydzień.

Anna Szafranko, Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.