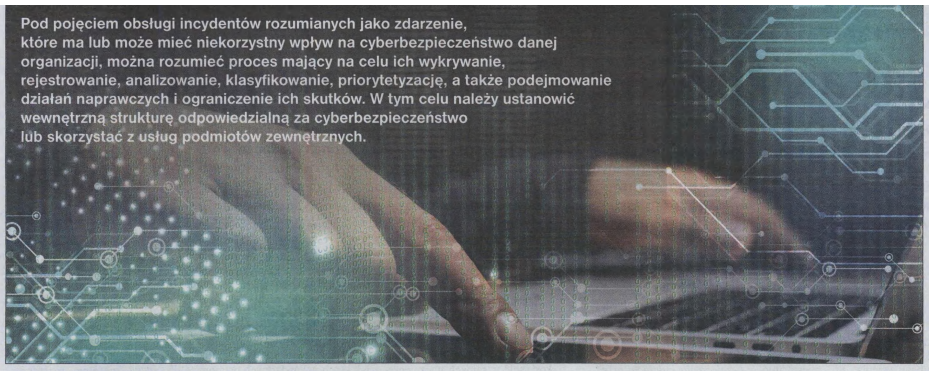

SKUTECZNOŚĆ OBSŁUGI INCYDENTU

Incydent cyberbezpieczeństwa na własne życzenie, czyli co można było zrobić lepiej

W przypadku tego incydentu bezpieczeństwa na żadnym z etapów jego obsługi nie pojawili się hakerzy, żądanie okupu lub przynajmniej złośliwe oprogramowanie. Zamiast tego doszło do przypadkowego ujawnienia danych klientów i pracowników spółki, a także klientów i pracowników jej kontrahentów. Co istotne, do powyższego doszło w taki sposób, że uległy one rozpowszechnieniu w internecie.

Co najgorsze, o całym zdarzeniu zarząd spółki dowiedział się przez przypadek. Po prostu jeden z pracowników odebrał telefon od nieznajomej osoby, która opowiedziała o swoim odkryciu.

Zapomnieć o ryzyku czy nim zarządzić

Po uzyskaniu takiej informacji większość zarządów spółek poszkodowanych w opisany sposób mogłaby zadać sobie pytanie, czy przypadkiem nie przeczekać i liczyć na to, że nikt więcej o zdarzeniu się nie dowie. Roztropność jednak nakazywałaby skonsultowanie tej kwestii pod kątem prawnym oraz technicznym.

W pierwszym przypadku warto bowiem sprawdzić, czy zatajenie informacji przed właściwymi organami, klientami i kontrahentami nie jest związane z kolejnymi negatywnymi skutkami, tym razem natury prawnej.

W drugim z kolei należałoby zabezpieczyć się przed następnym tego rodzaju zdarzeniem.

Gdzie szukać pomocy

Na tym etapie przedsiębiorca napotyka jednak kolejne przeciwności. Nie wie bowiem, u kogo mógłby szukać takiej pomocy.

Co prawda firmowy informatyk oferuje pomoc kolegi, który podobno zna się na takich sprawach, a jeden z członków zarządu namawia do skorzystania z usług kancelarii swojego bratanka, ale czy aby na pewno są to eksperci, którzy będą w stanie pomóc spółce?

Gdy czas działa na niekorzyść

Po tym jak stracono kolejny dzień na tego rodzaju rozważania, na profilu internetowym spółki jednego z portali społecznościowych pojawiają się wpisy z linkami do artykułów, jakie opublikowano na popularnych stronach zajmujących się cyberbezpieczeństwem. Tematem każdego z nich jest wyciek danych ze spółki, do której z każdą godziną zwraca się coraz więcej zaniepokojonych klientów, pracowników, kontrahentów oraz mediów z pytaniami na temat incydentu. Spółka niestety wciąż nie posiada kluczowych informacji na temat tego, co tak naprawdę się wydarzyło.

W artykułach i postach natomiast można przeczytać, że prezes Urzędu Ochrony Danych Osobowych (PUODO) na pewno powinien zająć się sprawą i wszcząć kontrolę w spółce, a klienci i kontrahenci prawdopodobnie wystąpią wobec spółki z roszczeniami odszkodowawczymi. Niemal w każdym z nich zwraca się także uwagę na to, że spółka nie reaguje na sytuację, co zdaniem autorów artykułów i postów tylko pogarsza jej sytuację.

Gdyby tego było mało, do spółki dochodzą informacje, że co bardziej zaciekawieni specjaliści od bezpieczeństwa znaleźli podatność, która nadal umożliwia zapoznanie się z danymi spółki, co oznacza, że incydent nadal trwa.

Co można było zrobić lepiej

W pierwszej kolejności należy podkreślić, że skuteczne zarządzanie ryzykiem w takim przypadku wymaga od przedsiębiorców uprzedniego wdrożenia systemu zarządzania bezpieczeństwem przynajmniej dla tych systemów informacyjnych, które są wykorzystywane przez nich do świadczenia usług.

W praktyce oznacza to co najmniej zapewnienie odpowiedniej i kompleksowej obsługi incydentów rozumianych jako zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo danej organizacji. Z kolei pod pojęciem obsługi takich incydentów można rozumieć proces mający na celu ich wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, a także podejmowanie działań naprawczych i ograniczenie ich skutków.

W tym celu należy ustanowić wewnętrzną strukturę odpowiedzialną za cyberbezpieczeństwo lub skorzystać z usług podmiotów zewnętrznych. W drugim z powyższych przypadków niezbędne byłoby przeprowadzenie weryfikacji, czy ewentualny usługodawca spełnia warunki organizacyjne i techniczne pozwalające na zapewnienie przedsiębiorcy cyberbezpieczeństwa, np. czy stosuje zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

Trzecim rozwiązaniem z kolei jest wykupienie odpowiedniej polisy, w ramach której zostanie m.in. zapewniona obsługa incydentu przez podmioty wynajęte przez ubezpieczającego oraz pokryte koszty obsługi prawnej, ochrony dobrego imienia, odzyskania utraconych danych, śledztwa oraz zawiadomienia właściwych organów.

Zespoły obsługi incydentów o charakterze doraźnym

Ostatnie z przedstawionych powyżej rozwiązań będzie korzystne przede wszystkim z perspektywy drobnych i średnich przedsiębiorców, którzy ze względów finansowych nie byliby w stanie zapewnić sobie usług dedykowanego personelu oraz sprzętu teleinformatycznego odpowiedniej klasy.

Dodatkowo należy podkreślić, że poza specjalistami od cyberbezpieczeństwa obsługa incydentów wymaga wsparcia prawnego oraz medialnego (ochrony wizerunku). Wsparcie prawne ma bowiem pozwolić na odpowiednią kwalifikację incydentów pod kątem m.in. ochrony danych osobowych (np. czy incydent podlega zgłoszeniu do prezesa Urzędu Ochrony Danych Osobowych, czy też nie) oraz sporządzenie rekomendacji w zakresie potencjalnych działań następczych, jak np. zawiadomienie o podejrzeniu popełnienia przestępstwa, wypowiedzenie umów nierzetelnym podwykonawcom lub obrona interesów przedsiębiorcy dotkniętego incydentem w przypadku zaistnienia ryzyka wystąpienia wobec niego z roszczeniami ze strony kontrahentów lub konsumentów.

Nie bez znaczenia pozostanie także ocena o charakterze prawno-technicznym w zakresie tego, czy przedsiębiorca dotknięty incydentem w jakimś stopniu nie dopuścił się naruszenia przepisów obowiązującego prawa, np. poprzez brak wdrożenia środków zaradczych, które są odpowiednie i zapewniające stopień bezpieczeństwa odpowiadający stwierdzonemu ryzyku.

Podsumowanie

Podsumowując, należy podkreślić, że skuteczność działań zewnętrznego oraz doraźnego zespołu obsługi incydentów (*ad hoc*) będzie uzależniona od tego, czy dany przedsiębiorca wdrożył w ramach swojej organizacji określone zasady działania. Do powyższego należy zaliczyć np. obowiązek zgłaszania incydentów wewnątrz organizacji oraz odpowiednimi kanałami zarządczymi najszybciej, jak to jest możliwe, a także zobowiązanie kontrahentów, podwykonawców i pracowników (niezależnie od podstawy, na jakiej zostali zatrudnieni) do odnotowywania oraz zgłaszania takich zdarzeń, jakie mogą wynikać np. z nieskutecznych zabezpieczeń, błędów ludzkich, naruszenia bezpieczeństwa fizycznego pomieszczeń oraz braku nadzoru nad systemami informacyjnymi. Bardzo pomocne mogą się okazać także takie działania jak sporządzenie wewnętrznego wzoru formularza do zgłaszania zdarzeń mogących stanowić incydenty (dot. pracowników i kontrahentów) oraz procedury postępowania w przypadku zaistnienia takiego zagrożenia, a także procedury dyscyplinującej pracowników oraz kontrahentów w razie naruszenia obowiązków dot. zgłoszenia w/w zdarzeń.

Dodatkowo rekomendowane jest opracowanie przez przedsiębiorcę zasad przekazywania pracownikom oraz kontrahentom, w tym podwykonawcom, informacji zwrotnych dotyczących zgłoszonych zdarzeń, a także zasad przekazywania wniosków z badania zdarzenia uznanego za incydent do innych podmiotów w łańcuchu dostaw.

Paweł Gruszecki
counsel w praktyce IP&TMT
w Domański
Zakrzewski Palinka sp.k.

O autorze. Specjalizuje się w obsłudze prawnej projektów wymagających wiedzy z zakresu prawa IT, ochrony danych osobowych, cyberbezpieczeństwa, prawa autorskiego, prawa mediów oraz prawa telekomunikacyjnego. Kieruje obsługą prawną projektów dostosowania operatorów usług kluczowych. Posiada duże doświadczenie w obsłudze dostawców usług internetowych, a także operatorów telekomunikacyjnych.