Maciej Gawroński, Radca Prawny; Piotr Biernatowski, Adwokat;
Michał Ćwiakowski, Adwokat, Kancelaria Gawroński & Partners s.k.a.

Ochrona danych osobowych

i (cyber)bezpieczeństwo sektora energetycznego

Czy atak socjotechniczny na jeden adres email pracownika podmiotu sektora energetycznego zagraża cyberbezpieczeństwu? Jeśli jest nieskuteczny, to pewnie nie. A jeśli zaatakowanych zostanie pięć tysięcy adresów? Wtedy to już nie ryzyko, tylko statystyka.

Sektor energetyczny tradycyjnie przywiązywał niedużą wagę do ochrony danych osobowych równocześnie chlubiąc się bezpieczeństwem automatyki przemysłowej (OT), jako elementu bezpieczeństwa infrastruktury krytycznej. Z tym że to ostatnie było trudno sprawdzić, z uwagi na tajność informacji w tym zakresie. Tę sielankę zakończyły dwa unijne akty - RODO i tzw. Dyrektywa NIS, wdrożona w Polsce ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC). Bardzo istotnym elementem zapewnienia cyberbezpieczeństwa w myśl KSC jest obsługa i zarządzanie incydentami bezpieczeństwa. RODO również przykłada wielką wagę do tego samego obszaru. W sektorze energetycznym są już pierwsze ofiary lekceważącego i silosowego podejścia do ochrony danych osobowych i ukrywania incydentów bezpieczeństwa danych osobowych. Z chwilą upływu terminu na wdrożenie KSC, lista ofiar zapewne się wydłuży i to nie tylko wśród personelu operatorów usług kluczowych sektora energetycznego.

Podmioty sektora energetycznego operatorami usług kluczowych

Wiele podmiotów szeroko rozumianego sektora energetycznego otrzymało decyzję o uznaniu za operatora usługi kluczowej. Podmioty, które tej decyzji nie otrzymały, nie mogą jednak odetchnąć z ulgą, gdyż zapewne znajdą się w drugiej lub trzeciej linii, na które naturalnie narzucony zostanie formalny standard zarządzania cyberbezpieczeństwem przez podmioty z pierwszej linii - operatorów usług kluczowych. *De facto*, dostawcy zewnętrzni, mający wpływ na świadczenie usług kluczowych, zobowiązani są do zapewniania cyberbezpieczeństwa na poziomie nieodbiegającym od tego narzuconego operatorom usług kluczowych. Jednym z podstawowych środków techniczno-organizacyjnych mających na celu zapewnienie bezpieczeństwa systemom informatycznym wykorzystywanym do świadczenia usług kluczowych jest zapewnienie bezpieczeństwa i ciągłości dostaw usług, od których ta usługa kluczowa zależy. Należy się zatem spodziewać wzrostu poziomu wymagań w obszarze cyberbezpieczeństwa, stawianych dostawcom zewnętrznym przez operatorów usług kluczowych.

Incydent w KSC i w RODO

Zarówno KSC, jak i RODO opierają się na wspólnych filarach wiedzy o bezpieczeństwie informacji i ciągłości działania. KSC kładzie większy nacisk na ciągłość działania, a RODO na poufność informacji. Jednak mylą się ci specjaliści bezpieczeństwa, którzy na tej podstawie lekceważą ochronę danych osobowych „przekazując ją" inspektorom ochrony danych (tzw. IOD-om).

Ustawa definiuje cyberbezpieczeństwo jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Incydent, z kolei, jest zdarzeniem, które ma lub może mieć negatywny wpływ na cyberbezpieczeństwo. Istota incydentu w rozumieniu KSC nie różni się bardzo od naruszenia ochrony danych osobowych. Jeżeli incydent jest poważny, tzn. powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej, operator obowiązany jest do zaraportowania incydentu do CSIRT. Analogicznie należy raportować naruszenia ochrony danych osobowych do PUODO.

Zintegrowane zarządzanie incydentami

Proces zarządzania bezpieczeństwem, jak i w szczególności proces zarządzania incydentami powinien być zintegrowany i na każdym jego etapie powinien uczestniczyć dział bezpieczeństwa. Zakwalifikowanie incydentu jako naruszenia ochrony danych osobowych zasadniczo nie może zwalniać działu bezpieczeństwa od oceny ryzyka / oceny wpływu incydentu na cyberbezpieczeństwo i ciągłość działania organizacji i pod-

jęcia działań, które takie ryzyko zmitygują, jeśli jest to możliwe.

Doradzając w obszarze ochrony danych osobowych w sektorze energetycznym, w tym w szczególności prowadząc audyty postępowań w sprawie incydentów ochrony danych osobowych, jak też oceniając stopień przygotowania operatorów usług kluczowych do realizacji obowiązków KSC, spotykamy się najczęściej z niewielkim stopniem zintegrowania działań związanych z ochroną informacji w obszarze ochrony danych osobowych oraz cyberbezpieczeństwa (a już zupełnie w kwestiach ochrony tajemnicy przedsiębiorstwa).

Równocześnie, podobnie jak w obszarze compliance (antykorupcja, przeciwdziałanie mobbingowi i molestowaniu seksualnemu, powoływanie się na wpływy, odpowiedzialność podmiotów zbiorowych, itp.), zbyt często sprawdza się życiowa prawda, iż „Szaleństwem jest żądać od filozofa, aby żył według głoszonych przez siebie zasad", co po prostu oznacza, że osoby odpowiedzialne za wdrażanie w organizacjach pewnych zasad, same się do nich nie stosują. Napotkaliśmy na przykłady sprzeniewierzania powierzonych danych osobowych, ukrywania incydentów przed PUODO, niszczenia logów, nie mówiąc już o niestosowaniu procedur przechowywania logów, dzielenia wiedzy na prywatną i służbową, etc.

Podejścia w przypadku wdrażania nowych regulacji są dwa. Pierwsze jest czysto „papierkowe" i polega na formalnym, a niekoniecznie praktycznym, spełnieniu wymogów regulacyjnych. Drugie podejście to faktyczne wdrożenie regulacji w sposób przemyślany, poparty refleksją co do przyczyn i powodów wprowadzenia regulacji, a także ich celu. W przypadku KSC, pierwsze podejście nie ma najmniejszego sensu. Pomijając fakt, że nie zwolni ono operatora usługi kluczowej z odpowiedzialności administracyjnej za niewdrożenie wymogów ustawy, to przede wszystkim nie zapewni mu cyberbezpieczeństwa. A cyberbezpieczeństwo, to nie tylko „spokój w relacjach z regulatorem", ale przede wszystkim ciągłość i bezpieczeństwo biznesu oraz mitygant ryzyka strat i kosztów związanych z incydentami.

Wymogi i filozofia KSC oraz RODO przenikają się. Dotyczy to przede wszystkim wymogów związanych z identyfikacją, raportowaniem i zarządzaniem incydentami. W każdej organizacji objętej tymi regulacjami, konieczne jest zapewnienie procesu tzw. projektowania bezpieczeństwa. W przeciwnym razie, przy najbliższym incydencie, którego nie uda się ukryć, w najlepszym wypadku trzeba będzie przejść do procesu szukania nowej pracy. A czy incydent uda się ukryć? Zwykle udaje się co najwyżej nieco odroczyć jego publiczną wiwisekcję.

W naszej praktyce wdrażamy i weryfikujemy wdrożenie RODO, wdrażamy regulacje bezpieczeństwa informacji, audytujemy sposób obsługi incydentów bezpieczeństwa, audytujemy gotowość do wdrożenia ustawy o krajowym systemie bezpieczeństwa. Doświadczenia z tych działań prowadzą do jednego wniosku - w obecnych czasach więcej korzyści przynosi paranoja niż lekceważenie i fanfaronada. Czy da się zapewnić cyberbezpieczeństwo i ochronę danych? To ciekawe pytanie. Da się natomiast zapewnić proces cyberbezpieczeństwa i bezpieczeństwa danych osobowych, o ile potraktuje się te obowiązki poważnie.

Skutki incydentów i wsparcie zewnętrzne

Zarządzanie incydentem jest procesem dynamicznym. Faktem jest, że w przypadku wystąpienia incydentu nie ma czasu na kompletowanie zespołu posiadającego kompetencje do zarządzania tą sytuacją. Taki zespół należy po prostu mieć. Nieprawidłowe wdrożenie zabezpieczeń, jak również nieprawidłowe zarządzanie incydentami pociąga za sobą poważne skutki i ryzyko odpowiedzialności zarówno dla organizacji, członków zarządu, jak i poszczególnych pracowników, do których zadań należą w/w zagadnienia. Znane nam są przypadki, gdy naruszenia w zakresie obsługi incydentu stanowiły podstawę dyscyplinarnego zwolnienia z pracy. Biorąc pod uwagę powagę materii, z którą się mierzymy należy uznać, że nieprawidłowości w tym zakresie stanowią poważne naruszenie obowiązków pracowniczych u osób, które w strukturze organizacji są za nie odpowiedzialne. Obok konsekwencji pracowniczych, incydent, to także straty biznesowe związane z przerwami w świadczeniu usług, cywilnymi roszczeniami osób i podmiotów nim dotkniętych oraz odpowiedzialnością administracyjną. Wszystko zależy od jego charakteru, skutków oraz bardzo często sposobu i jakości zarządzenia nim.

Dlatego, w zakresie wdrożenia i oceny procesów związanych z zapewnieniem cyberbezpieczeństwa i ochrony danych osobowych, warto rozważyć wsparcie niezależnego, zewnętrznego doradcy. Nie chodzi tylko o kwestie implementacji i audytu ogólnego, ale niekiedy także zarządzenie konkretnymi zdarzeniami, np. skutkami incydentu, który w organizacji wystąpił. Najlepiej jeżeli taki doradca posiadał będzie doświadczenie i kompetencje w zakresie obsługi incydentów na styku ochrony danych osobowych oraz bezpieczeństwa informacji.

Zaangażowanie zewnętrznego podmiotu pozwala także zarządzić potencjalnym konfliktem interesów wewnątrz organizacji. Jeżeli operator zapewnia bezpieczeństwo, w tym cyber, i obsługę incydentów wewnętrznie, zawsze istnieje ryzyko wystąpienia konfliktu interesów, skoro to pracownicy są za nie odpowiedzialni, a jednocześnie dokonują ich oceny. Ktoś w organizacji odpowiedzialny jest za zapewnienie systemu bezpieczeństwa, a wystąpienie incydentu to przecież porażka tego sytemu. Pytanie czy oceny tego systemu można i powinno się w takiej sytuacji dokonywać wewnętrznie. Ustawodawca dostrzega to zagadnienia i co nie zdarza się wcale często, narzuca operatorom usług kluczowych obowiązkowe, regularne audyty bezpieczeństwa.

Zapraszamy do kontaktu:
Gawroński & Partners
Al. Jana Pawła II 12 | 00-124 Warszawa
Tel. +48 22 243 4953
info@gppartners.pl