aut. Bartosz Józefiak 05.07.2016

NADCHODZĄCA ZMIANA W ODPOWIEDZIALNOŚCI ZA CYBERBEZPIECZEŃSTWO INFRASTRUKTURY KRYTYCZNEJ

Dziś operatorzy infrastruktury krytycznej mogą czuć się bezpieczni, jeżeli chodzi o prawne konsekwencje związane z cyberatakiem. To jednak już wkrótce się zmieni. Dwa nowe zestawy unijnego prawa, czyli ogólne rozporządzenie o ochronie danych i dyrektywa NIS oznaczają, że szefowie firm zostaną pociągnięci do odpowiedzialności, jeżeli nie dołożyli wszelkich starań by zapobiec atakowi – największym błędem polskich firm jest kompletny brak procedur w razie incydentu – mówią eksperci.

- Nie mamy żadnych regulacji prawnych związanych z cyberbezpieczeństwem – mówi Marcin Maruta z kancelarii prawnej Maruta Wachta, ekspert od prawa w cyberprzestrzeni. Aspekty prawne z tym związane dopiero teraz pojawiają się na horyzoncie zainteresowań przedsiębiorców. Mamy co prawda regulacje dotyczące zarządzania kryzysowego, ale nie mamy regulacji dotyczących cyberobrony przedsiębiorstw - dodał ekspert.

Specjalista wyjaśniał prawne zagadnienia cyberbezpieczeństwa podczas konferencji „Cyberbezpieczeństwo przemysłu i infrastruktury krytycznej" zorganizowanej przez Kaspersky Labs dla przedstawicieli firm zarządzających IK.

- Gdyby państwo nie mieli żadnych zabezpieczeń przed cyberatakiem, to w sądzie nie obronilibyście się. Ciąży na was obowiązek dołożenia należytej staranności. Nie byłoby jednak łatwo wskazać, gdzie kończy się „należyta staranność".

Ochrony danych osobowych nie można zlecić na zewnątrz

Co grozi operatorom infrastruktury krytycznej, którzy nie inwestują w cyberochronę? Dzisiaj tak naprawdę niewiele. Brak prawnych uregulowań tej kwestii oznacza, że pociągnięcie kogoś do odpowiedzialności za skutki cyberataku jest niezwykle trudne. W przypadku włamań zwalnia się CIO firmy ze względu na brak procedur, które mogły uchronić przedsiębiorstwo przed negatywnym skutkiem ataku. Ważne jest, by jak najszybciej powiadomić organy ścigania – najlepiej nie dzwoniąc na 997, tylko od razu kontaktując się z komórką policji i ABW, które odpowiadają za cyberprzestępstwa.

- W Polsce nie ma ustawodawstwa regulującego systemy ochrony cyberprzestrzeni. Firmy muszą obserwować zmieniające się przepisy i zasady ochrony infrastruktury krytycznej zawarte w Narodowym Programie IK 2015. Standardy służące zapewnieniu sprawnego funkcjonowania IK, dobre praktyki i rekomendacje przygotowało Rządowe Centrum Bezpieczeństwa. Warto się z nimi zapoznać – wyjaśniał Marcin Maruta.

Sektor finansowy jest jedynym, który ma konkretne wytyczne dotyczące cyberbezpieczeństwa. Komisja Nadzoru Finansowego wydaje rekomendacje na bardzo szczegółowym poziomie. To właśnie z sektora finansowego należy brać przykład w kwestii cyberbezpieczeństwa.

Sytuację zmieni wejście w życie regulacji dotyczących ochrony danych osobowych, czyli ogólnego rozporządzenia o ochronie danych (General Data Protection Regulation - GDPR). Przepisy zostały już zaakceptowane przez Parlament Europejski i zaczną obowiązywać od połowy 2018 r. Instytucje już teraz powinny zacząć przygotowywać się do ich wdrożenia. Nowe prawo wprowadza bowiem bardzo wysokie kary umowne związane z nieprzestrzeganiem przepisów.

Na firmy będzie nałożony obowiązek zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego (w naszym przypadku GIODO) oraz przez podmioty przetwarzające do administratorów danych. Jedną z najważniejszych nowości - budzącą największe emocje - jest możliwość nakładania kar pieniężnych przez organ nadzorczy (GIODO) za nieprzestrzeganie przepisów o ochronie danych. Rozporządzenie opisuje warunki nakładania kar w wysokości od 10 do 20 milionów euro lub od dwóch do czterech proc. całkowitego rocznego światowego obrotu przedsiębiorstwa, które nie zastosuje się do nowych wytycznych.

- Skończy się niezwykle częsta praktyka siedzenia cicho i ukrywania incydentów. Przestanie być zabawnie – ironizuje Marcin Maruta. - Działy dotyczące bezpieczeństwa będą musiały włączyć się w ochronę danych osobowych. Nie da się tego zadania zlecić na zewnątrz. To będzie podstawowy obowiązek firmy.

Procedury to podstawa

Jeszcze więcej w kwestii cyberbezpieczeństwa zmieni unijna dyrektywa NIS (Network and Information Security), która ma na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii Europejskiej. Nowe prawo zacznie najpewniej obowiązywać w ciągu dwóch – trzech lat. – Operatorzy kluczowych usług już powinni zacząć o niej myśleć – mówi Marcin Maruta. – Proces wdrożenia przepisów w firmie zajmie co najmniej rok.

Nowe prawo sprawi, że firmy będą miały obowiązek raportować incydenty do krajowych organów (W Polsce – do Narodowego Centrum Cyberbezpieczeństwa). Regulator będzie mógł żądać udzielania informacji i wydawać wiążące wskazówki w zakresie działań zmierzających do zapewnienia bezpieczeństwa. Na razie polska ustawa o cyberbezpieczeństwie dopiero się tworzy. Przepisy pojawią się do końca roku. - Ale już teraz nie ma na co czekać. Firmy mogą podpatrywać rozwiązania zapisane w założeniach strategii cyberbezpieczeństwa i zaleceniach RCB – tłumaczy ekspert.

Co jest jednak największym błędem firm? Według Marcina Maruty to brak procedur i wytycznych w razie cyberataku. - Prawnicy są wzywani dopiero, kiedy już dojdzie do incydentu. Okazuje się nagle, że zarząd firmy nie ma pojęcia, co robić. Czy powiadamiać klientów, policję, jeśli tak, to którą? Jeśli jakakolwiek kontrola będzie sprawdzała efekty cyberataku, zwróci uwagę na jedną rzecz – czy w firmie były procedury i czy realizowano je krok po kroku. Problemem nie jest włamanie, problemem jest brak procedur. Za takie rzeczy lecą głowy CIO i zarządu – tłumaczy specjalista od prawa w cyberprzestrzeni.

Każde przedsiębiorstwo musi dysponować kilkoma podstawowymi dokumentami, wśród nich są m.in polityka bezpieczeństwa, polityka postępowania w razie ataku. - Być może to papierologia, ale potrzebna – dodaje ekspert. Ważne jest też szkolenie pracowników, co pozwoli uniknąć kompromitujących pomyłek zagrażających bezpieczeństwu. Firmy muszą już teraz poważnie myśleć o wdrożeniu GDPR i dyrektywy NIS. - To są absolutnie podstawowe zadania w zakresie cyberbezpieczeństwa – podsumowuje Marcin Maruta.

Czytaj też: Stuxnet nie zniknął. Infrastruktura krytyczna nadal narażona na cyberatak