aut. Andrzej Kozłowski 24.05.2019

USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA POPRAWI KONKURENCYJNOŚĆ FIRM [WYWIAD]

O obowiązkach przedsiębiorców wynikających z Ustawy o krajowym systemie cyberbezpieczeństwa, jej wpływie na konkurencyjność firm oraz roli operatorów usług kluczowych mówi w wywiadzie dla CyberDefence24.pl kierownik projektu w Zespole Wsparcia Sprzedaży EXATEL, Paweł Deyk.

Andrzej Kozłowski: W skład KSC mają wejść tzw. operatorzy usług kluczowych i usług cyfrowych? Jakie to będą przedsiębiorstwa?

Paweł Deyk: Zacznijmy od dostawców usług cyfrowych. Są to organizacje z siedzibą w Polsce, które świadczą usługi cyfrowe. Wśród nich mogą się znaleźć np. internetowe platformy handlowe, wyszukiwarki, czy operatorzy usług chmurowych.

Z kolei operatorzy usług kluczowych to przedsiębiorstwa, które świadczą swoje usługi w jednym z sześciu obszarów krytycznych z punktu widzenia gospodarki państwa: energii, transporcie, bankowości, ochronie zdrowia, zaopatrzenia w wodę pitną (wraz z jej dystrybucją) oraz infrastruktury cyfrowej.

To, że działamy w wyżej wymienionych sektorach nie oznacza jeszcze, że automatycznie będziemy podlegać pod ustawę o KSC. Jest jeszcze jeden dodatkowy warunek – skala działalności. Dlatego nie każde z przedsiębiorstw będzie uznane przez właściwą instytucje (ministerstwa sektorowe oraz KNF) za operatora usługi kluczowej.

Na jakich zasadach będą wyznaczani i do kiedy?

Dwa warunki już wymieniłem. To świadczenie usługi w jednym z wymienionych wcześniej sektorów gospodarki oraz skala działalności. Wynika to z wykazu określonego przez Radę Ministrów. I tak np. przy transporcie lotniczym mówimy o skali minimum 500 tys. pasażerów rocznie a przy uzdatnianiu wody o minimum 500 tys. podłączonych mieszkańców. Czyli mówimy o organizacjach, których niewłaściwe funkcjonowanie będzie miało dużą konsekwencję dla gospodarki lub dużej grupy osób. Ostatnim warunkiem jest wymóg, aby świadczenie usługi kluczowej zależało od systemów informacyjnych.

O uznaniu za dostawcę usługi cyfrowej decydować będzie wyłącznie faktyczny charakter prowadzonej działalności i jej rozmiar, a nie decyzja któregoś z organów. Pamiętajmy, że również podmioty publiczne, takie jak szkoły, czy urzędy gmin zostały objęte ustawą i stanowią najliczniejszą grupę objętą ustawą o KSC.

Co zaś się tyczy harmonogramu. Decyzje te miały być wydane do 9 listopada 2018 r. Ale odpowiednie

postępowania administracyjne trwają nadal.

Ile ich będzie? Czy ich lista będzie udostępniona publicznie?

Wykaz wszystkich operatorów usług kluczowych prowadzi Ministerstwo Cyfryzacji. Jednak ich lista nie będzie publicznie dostępna. Szacunkowa liczba podawana przez resort cyfryzacji to ponad 500 operatorów usług kluczowych. Z ostatnich doniesień medialnych wynika, że decyzje otrzymało już ok. 70 podmiotów. Ciężko oszacować natomiast ile podmiotów działa jako dostawca usług cyfrowych ze względu na brak szczegółowych informacji na temat klasyfikacji tych podmiotów.

Jakie obowiązki zostaną nałożone na podmioty gospodarcze, które zostaną objęte KSC i jakie są negatywne konsekwencje ich nie spełnienia? Czy przewidziane są jakieś kary?

Najbardziej surowe wymagania stawiane są operatorom usług kluczowych. Dostawcy usług cyfrowych nie mają już tylu obostrzeń. Natomiast podmioty publiczne otrzymały bardzo podstawowe wymagania.

I tak do najważniejszych obowiązków Operatorów Usług Kluczowych należą:

- wdrożenie systemu zarządzania bezpieczeństwem (z uwzględnieniem m.in. szacowania ryzyka, planów ciągłości działania, zbierania informacji o zagrożeniach i podatnościach systemów),
- zgłoszenie i obsługa incydentów (klasyfikacja, określenie wpływu na usługę kluczową, szacowanie skutków oddziaływania incydentu, zgłoszenie do właściwego CSIRT w ciągu 24 h oraz usunięcie podatności systemu),
- powołanie struktur wewnętrznych odpowiedzialnych za cyberbezpieczeństwa lub podpisanie umowy z podmiotem zewnętrznym świadczącym usługi,
- przeprowadzanie audytów bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej w ciągu roku od wydania decyzji. Później audyt ma mieć charakter cykliczny, raz na 2 lata,

Z kolei dostawcy usług cyfrowych mają obowiązek:

- stosować środki bezpieczeństwa proporcjonalne do ryzyka,
- podejmować czynności umożliwiające wykrywanie i analizowanie incydentów, a także podejmowanie działań naprawczych ograniczających skutki incydentu,
- zarządzać ciągłością działania w celu świadczenia usługi cyfrowej,
- zapewniać zgodność z zaleceniami, o których mowa w rozporządzeniu wykonawczym Komisji Unii Europejskiej (2018/151).
- zapewniać monitorowanie, audyt i testowanie systemów.

Natomiast podmioty publiczne mają obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, a także zarządzać incydentem zapewniając jego obsługę. Czas na zgłoszenie incydentu do właściwego CSIRT nie może przekroczyć 24 godzin od momentu wykrycia.

Istotnym elementem ustawy o KSC są kary pieniężne za zaniechanie lub niedopełnienie obowiązków. Chodzi tutaj przede wszystkim o brak dokumentacji, brak środków technicznych, nieusuwanie podatności, niezgłaszanie incydentów do CSIRT, brak audytu czy brak realizacji zaleceń pokontrolnych. W takich przypadkach mówimy o kwotach w wysokości od 1000 zł do nawet 1 000 000 zł za uporczywe łamanie przepisów.

Jakie największe problemy mogą mieć przedsiębiorcy z wypełnieniem obowiązków wynikających z KSC?

Dla wielu z podmiotów będą to zupełnie nowe obowiązki, które dotychczas nie były traktowane zupełnie poważnie. Systemy potrzebne do zabezpieczenia infrastruktury i danych nie należą do najtańszych, a specjalistów od cyberbezpieczeństwa brakuje nie tylko w Polsce, ale i na całym świecie. Zespoły wewnętrzne, które dotychczas zajmowały się tylko obsługą infrastruktury informatycznej, teraz otrzymają dodatkowe zadania. Konieczne będzie przeprowadzenie audytów, usystematyzowanie procedur, dokumentacji oraz przeprowadzenie solidnej analiza ryzyka. Do przeprowadzenia tych działań należy mieć kompetentny zespół, który dobrze rozumie specyfikę profilu organizacji.

Dodatkowo należy spodziewać się, że plany zakupowe zaczną w końcu zawierać elementy związane z bezpieczeństwem IT – systemy SIEM, antymalware, rozwiązania chroniące stacje końcowe czy służące do lepszego monitorowania infrastruktury. Nie jest to łatwe. Sam proces zakupu i wdrożenia odpowiednich rozwiązań technicznych przysporzy organizacjom wiele trudności.

Czy zapisami KSC mogą zostać również objęte MŚP?

Mikro i mali przedsiębiorcy są wyłączeni z klasyfikacji jako dostawcy usług cyfrowych. Jednak średnie przedsiębiorstwa (powyżej 50 pracowników lub powyżej 10 mln euro rocznego obrotu), które świadczą usługę cyfrową, będą objęte działaniem ustawy. W przypadku operatorów usług kluczowych nie są przewidziane żadne wyłączenia związane z wielkością organizacji.

W jaki stopniu KSC pozwala na wykorzystanie wsparcia zewnętrznych specjalistów cyberbezpieczeństwa?

Jest to jak najbardziej możliwe. Zarówno w części audytowej, jak i przy bieżącym monitorowaniu i obsłudze incydentów warto wykorzystać doświadczenie i zasoby, którymi dysponują przedsiębiorcy z branży cyberbezpieczeństwa. Dzięki odpowiednim umowom o poufności informacji podpisanym z firmą zewnętrzną, a także posiadaniu przez nią certyfikatów potwierdzających spełnianie norm i standardów, możemy z czystym sumieniem outsourcować większość zadań poza struktury własnej organizacji. Najważniejszy jest odpowiedni dobór partnera, który powinien budzić zaufanie i charakteryzować się dobrą renomą na rynku usług cyberbezpieczeństwa. W najbliższym czasie należy spodziewać się zalewu nowych przedsiębiorstw, bez doświadczenia i odpowiedniego zaplecza, które będą oferować usługi Security Operations Center w celu spełnienia wymagań stawianych przez Ustawę o Krajowym Systemie Cyberbezpieczeństwa.

Czy KSC nie wpłynie negatywnie na konkurencyjność firm?

Moim zdaniem ustawa wpłynie wręcz pozytywnie na konkurencyjność organizacji, które potraktują poważnie zawarte w niej wymogi. Wiem, że ustawa wymaga pewnych nakładów finansowych oraz wysiłku, który może być postrzegany jako ciężar. Pamietajmy jednak, że w nowoczesnej gospodarce opartej na wiedzy i innowacjach najcenniejszymi zasobami są dane, które gromadzi organizacja (know-how, tajemnice handlowe, itd.). Zabezpieczenie tego typu zasobów powinno być priorytetem dla każdego przedsiębiorstwa, które chce się rozwijać i wyprzedzać konkurencję. Kolejnym ważnym aspektem jest reputacja firmy, która może zostać łatwo zachwiana przez ogłoszenie informacji o ataku hakerskim czy wycieku danych, który nie został powstrzymany.

W jaki sposób EXATEL może pomóc firmom spełnić obowiązki wynikające z KSC?

Posiadamy kompetencje w świadczeniu usług bezpieczeństwa IT od kilku lat rozwijając zespół specjalistów Security Operations Center, który pracuje w trybie 24/7/365 i posiada kilkudziesięciu specjalistów podzielonych na 3 linie wsparcia.

Możemy kompleksowo wesprzeć organizację w realizacji zadań ustawowych. Zaczynając od

pierwszego etapu czyli przeglądu zgodności z wymaganiami ustawy KSC. W nim określamy potencjalne braki do uzupełnienia i uświadamiamy osoby zarządzające organizacją o skali wyzwań związanych z nowymi regulacjami. Ale także w kolejnych etapach. Wdrażamy systemy bezpieczeństwa i świadczymy usługi utrzymania i zarządzania nimi. Swoim partnerom dajemy możliwość skorzystania z wsparcia specjalistów SOC w różnych modelach, np. angażując 1 linię SOC do obserwowania alertów generowanych przez systemy SIEM klientów, czy umożliwiając z korzystania z zaawansowanych usług cyberbezpieczeństwa (np. analiza wsteczna oprogramowania, tworzenie reguł korelacyjnych) wykonywanych przez specjalistów linii 3. Nasze usługi zawsze są odpowiedzią na realne potrzeby organizacji.

Mocno stawiamy również na edukację i uświadamianie naszych potencjalnych partnerów o tym, jak ważne jest traktowanie bezpieczeństwa IT. To właśnie po to organizujemy takie konferencje jak czerwcowa EXATEL Security Days, gdzie dyskutujemy o praktycznej stronie cyberbepieczeństwa. Bo dziś to temat bardzo ważny dla wszystkich - zarówno dla małych organizacji, jak i wielkich spółkek notowanych na giełdzie.

Paweł Deyk - Kierownik projektu w Zespole Wsparcia Sprzedaży EXATEL