aut. Andrzej Kozłowski 17.07.2018

USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA OKIEM EKSPERTÓW [ANALIZA]

Ustawa o krajowym systemie cyberbezpieczeństwa to najważniejszy akt prawny dotyczący cyberbezpieczeństwa w Polsce. Powinna stać się fundamentem budowy skutecznego systemu cyberbezpieczeństwa. CyberDefence24.pl postanowił zapytać ekspertów co myślą, na temat tego dokumentu prawnego. Opinie są podzielone od mocno krytycznych do umiarkowanego optymizmu.

Ireneusz Piecuch – partner w CMS Cameron McKenna

Czasami ludzie mówią „lepiej późno niż wcale" ale zastanawiam się czy to powiedzenie można byłoby odnieść do nowej ustawy o krajowym systemie cyberbezpieczeństwa. Na plus należy zaliczyć to, ze problem cyberbezpieczeństwa - moim zdaniem największe wyzwanie cyfrowej transformacji - został w ogóle zaadresowany. Zdecydowanym minusem tej ustawy jest jej konstrukcja będąca świadectwem archaicznego myślenia o roli i możliwości państwa w czasach IV rewolucji przemysłowej. Trzy państwowe CIRTy z bliżej nieokreślonym modelem finansowania, sztywne (żeby nie powiedzieć biurokratyczne) zasady współpracy i efemerycznie zarysowany system edukacji i certyfikacji nie wróża tej ustawie nic dobrego. Na przeciwko urzędnikom państwowym, bo tak to mniej więcej ma wyglądać, stają bowiem świetnie wyposażone w wiedzę i środki technologiczne zastępy hakerów wspieranych przez międzynarodowe konglomeraty przestępcze a niejednokrotnie przez inne państwa, które już lata temu zrozumiały ze cyberprzestrzeń jest kolejna arena zmagań o globalną dominację. Nawet państwa dużo bardziej zaawansowane technologicznie od nas zrozumiały już, że ochrona cyberprzestrzeni wymaga efektywnej współpracy zarówno w wymiarze globalnym (ustawa spełnia w tej mierze wymagania dyrektywy NIS ale nic poza tym) a także w wymiarze partnerstwa publiczno-prywatnego. I tu dochodzimy do sedna problemu. Dlaczego partnerstwo to miałoby zadziałać w newralgicznym obszarze cyberbezpiecznstwa, skoro od lat jest niechcianym dzieckiem kolejnych administracji ?

Robert Siudak – dyrektor ds. współpracy i realizacji projektów Instytutu Kościuszki

Ustawa o krajowym systemie cyberbezpieczeństwa była niezbędna nie tylko z powodu zobowiązań związanych z implementacją dyrektywy NIS, ale także rzeczywistych wyzwań – w 2018 roku prawie 40 milionowy kraj znajdujący się w coraz bardziej niepewnym otoczeniu geopolitycznym, wciąż nie posiadał systemu wymiany informacji o zagrożeniach w cyberprzestrzeni, nie licząc kilku sektorowych wyjątków godnych docenienia takich jak np. sektor bankowy.

W tym kontekście należy pozytywnie ocenić wskazanie podmiotów odpowiedzialnych za zbieranie oraz udostępnianie informacji o incydentach w polskiej cyberprzestrzeni (CSIRT NASK, CSIRT MON, CSIRT GOV). Jednocześnie powstaje pytanie czy ustanowione zostaną sektorowe zespoły cyberbezpieczeństwa, w praktyce sektorowe CSIRT-y, co umożliwiają zapisy ustawy. Biorąc pod

uwagę zarówno specyfikę określonych sektorów (np. energetycznego lub ochrony zdrowia) jak i kwestię wymiany informacji w ramach krajów członkowskich UE, wydaje się to pożądanym działaniem.

Największym mankamentem ustawy wydaje ilość zapisanych w niej środków budżetowych. W praktyce realizacja celów oraz założeń dokumentu może się rozbić o brak funduszy. Kwoty, a właściwie limity środków jakie zaplanowano na lata 2019 – 2027 są co najmniej niewystarczające. Odnosząc się np. do kwestii ustanawiania sektorowych zespołów cyberbezpieczeństwa, na pewno nie uda się tego uczynić w ramach przewidzianych limitów. W tym kontekście negatywnie należy także ocenić zapis dotyczący praktycznego „wyłączania cyberbezpieczeństwa" w wypadku przekroczenia limitów. Mowa wówczas o ograniczeniu monitorowania działalności operatorów kluczowych i dostawców usług cyfrowych, rezygnacji z ćwiczeń oraz działalności sektorowych CSIRT (jeśli w ogóle powstaną przy takich limitach!). Należy zapytać – kto zapłaci za cyberbezpieczeństwo? – jeśli nie zostaną wygospodarowane dodatkowe środki z budżetu na rzeczywistą budowę systemu cyberbezpieczeństwa, wówczas koszt ten będziemy ponosili wszyscy, zarówno obywatele jak i administracja, tyle, że w postaci strat związanych z cyberatakami.

Małgorzata Fraser – specjalistka ds. prywatności i analityczka bezpieczeństwa, członkini Internet Society

Założenia towarzyszące powstaniu ustawy są niewątpliwie słuszne. Według nich, ma ona przyczynić się do lepszego radzenia sobie na poziomie krajowym z cyberatakami i pomóc minimalizować straty w przypadku wystąpienia incydentów. Szkoda jednak, że ustawa powstała dopiero teraz, kiedy wymusił to obowiązek wdrożenia unijnej dyrektywy NIS. To niezbędny ruch w stronę systematyzacji działań w zakresie cyberobronności na poziomie państwowym - warto jednak podkreślić, że Polska zdecydowała się na niego bardzo późno. Mając na uwadze zdarzenia z 2017 roku, takie jak pojawienie się WannaCry czy NotPetya, a także szybko zmieniający się krajobraz zagrożeń, przede wszystkim ze względu na rosnącą liczbę urządzeń IoT - być może to ostatni dzwonek. Mocną stroną ustawy jest niewątpliwie konieczność stworzenia krajowej strategii cyberbezpieczeństwa. Pytanie jednak, jak ta strategia będzie zbudowana, a także jak będzie w praktyce wyglądało jej wdrażanie. Warto pamiętać, że kluczowe w wartościowaniu strategii jest nie tylko to, w jaki sposób została ona napisana, ale również to, czy jest adekwatna względem posiadanych przez kraj zasobów i czy rzeczywiście można ją wdrożyć, zatem - jej wymiar praktyczny. Dużym mankamentem ustawy są niewątpliwie zapisy dotyczące budżetowania. Na całym świecie wydatki na cyberbezpieczeństwo są coraz większe. Do stopniowego zwiększania budżetów wzywają organizacje przedsiębiorców, media, rozumieją to również same rządy – martwi więc, że w polskiej ustawie o Krajowym Systemie Cyberbezpieczeństwa budżetowanie jest zorganizowane „na sztywno". Stały poziom finansowania zapisano aż do 2027 roku. Czy naprawdę możemy w roku 2018 oceniać, jakiego budżetu na cyberbezpieczeństwo Polska będzie potrzebowała za 9 lat? Czy oznacza to, że rzeczywistość zagrożeń nie zmieni się?

Bardzo martwią również zapisy ustawy wskazujące na ograniczenie działań z zakresu cyberbezpieczeństwa, jeśli limit wydatków przewidziany w budżecie zostanie wyczerpany. W praktyce oznacza to, że po wyczerpaniu - przykładowo - środków w wysokości 404 tys. zł, jakie na cyberbezpieczeństwo chce przeznaczyć dany organ, nie będzie on już reagował na kolejne incydenty - co wówczas stanie się z bezpieczeństwem struktur, danych, a ostatecznie - obywateli?

Dr Łukasz Olejnik, niezależny ekspert cyberbezpieczeństwa i prywatności, https://Prywatnik.pl

Implementacja unijnej dyrektywy NIS ustawą o krajowym systemie cyberbezpieczeństwa to dobry, długo oczekiwany początek systemu cyberbezpieczeństwa. Podstawowe kwestie prawno-organizacyjne stają się uporządkowane. Gdy już są te podstawowe zasady, można zająć się kwestią faktycznych możliwości detekcji przypadków gdy faktyczny poziom cyberbezpieczeństwa będzie

niższy niż ten wymagany w NIS. Efektywność tych instrumentów wykrywająco-egzekwujących będzie jednym z testów działania systemu uregulowań.

Dobrym krokiem jest powołanie Zespołu do Spraw Incydentów Krytycznych, a także Pełnomocnika Rządu ds Cyberbezpieczeństwa, ale zawsze pozostanie pytanie kompetencje. Jednak jasna świadomość kto bierze systemową i polityczną odpowiedzialność za cyberbezpieczeństwo w kraju, sygnuje ją swoim nazwiskiem, jest dobra. Tylko czy osoba ta będzie miała narzędzia do działań? Ustalone na sztywno kwoty "kar maksymalnych" to potencjalny punkt ryzyka. Wysokość "kosztu" sprowadzenia zagrożenia dla życia i zdrowia ludzi lub dla bezpieczeństwa państwa w maksymalnej kwocie 1 mln zł stanie się przecież jednym z elementów motywujących do podejmowania (lub nie) działań. Kwota ta jest dużo niższa niż poziom "kar" wynikających z GDPR, w tej regulacji specyfika ryzyka jest jednak inna. Jednym wymogów Ustawy jest też obowiązek przeprowadzania audytów bezpieczeństwa systemów. Teraz mieć na uwadze - podobnie jak to niestety miało w przypadku RODO w Polsce - usługi w rodzaju "Audyt i Zgodność za 99 zł" nie były tolerowane.

Według Ustawy ma powstać nie tylko lista podmiotów objętych obowiązkami zapewniania odpowiedniego poziomu cyberbezpieczeństwa oraz wykazywania się tu odpowiedzialnością, ale też Strategia Cyberbezpieczeństwa RP. Nie ma wątpliwości, że tym razem uda się to zrobić. Pozostaje jednak kwestia zawartości i kompleksowości. Części obszaru cyberbezpieczeństwa NIS przecież nie obejmuje, trzeba więc wykazać cierpliwość i nadzieję że kiedyś powstanie świadomość i tego.

Mirosław Maj – prezes Fundacji Bezpieczna Cyberprzestrzeń

Trwa dyskusja dotycząca jakości tego aktu. W większości rozpoczynają się one stwierdzeniem „dobrze, że wreszcie jest". Często również kończą się takim stwierdzeniem. Zazwyczaj unikam tak dalece oportunistycznej oceny, ale tym razem przyłączam się do tych głosów. Przemawiają za tym dwie istotne przyczyny. Po pierwsze – o rzetelną ocenę jest bardzo trudno. W praktyce nie ma idealnego modelu referencyjnego, a często przywoływane rozwiązania w takich państwach jak Stany Zjednoczone, Wielka Brytania czy Izrael z trudem można przenieść na rodzimy grunt legislacyjny. Dyrektywa NIS była tylko drogowskazem. Szczegóły implementacyjne pozwalały na sporą dowolność. Nie ma też za bardzo gotowych rozwiązań, a tym bardziej standardów międzynarodowych, które jasno by wskazywały jak zorganizować system cyberbezpieczeństwa państwa. Ten obszar przez ostatnie kilkanaście lat był w praktyce pomijany w systemach legislacyjnych i dlatego rozwinęły się najróżniejsze podejścia wynikające z praktyki działań w poszczególnych państwach. Po prostu trzeba było coś organizować, aby „jakoś ciągnąć ten wózek". W efekcie na świecie mamy sytuację „co kraj to obyczaj". Drugi z powodów przyłączenia się do popularnych opinii o Ustawie to długoletnie zmęczenie materiału. O uporządkowaniu legislacyjnym tego obszaru rozmawiamy w Polsce od ponad dziesięciu lat. Pierwsze prace nad „Polityką Ochrony Cyberprzestrzeni RP" rozpoczęły się jeszcze w 2008 r. Długość prac nieraz wykraczała poza tytuł planowanego dokumentu. Polityka miała być na określone lata, a w połowie tego okresu dopiero kończyły się prace nad nią. Za chwilę zresztą rozpoczynane poprzez „nową ekipę", itd. Była to dość irytująca sytuacja. Dzisiaj potrzebujemy czegoś co nie będzie miało błędów krytycznych i po prostu zacznie być wdrażane. UoKSC spełnia te warunki.

Ustawa nie jest doskonała. Powiedziałbym, że fragmentami jest dobra, fragmentami dostateczna. Dobry jest system operacyjnej koordynacji opartej o trzy CSIRT-y krajowe. Dostateczny jednak jest zarys koordynacji na poziomie odpowiedzialności polityczno-strategicznej. Ma jednak ustawa tę zaletę, że jest, a więc może być wdrażana i poprawiana. To ostatnie jest działaniem koniecznym i powinno stanowić podstawowe założenie wszystkich, którzy włączają się w proces budowy systemu opisanego w ustawie.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa nie jest idealna. Pojawienie się jej to dopiero początek drogi. Myślę, że dość wyboistej. W okresie najbliższych 2–3 lat więcej o tym jak będzie

wyglądał ten system zdecydują praktyczne ustalenia pomiędzy najważniejszymi graczami w tym systemie, niż czytanie konkretnych zapisów. Te powinny być tylko wskazówkami. Tylko aktywność i praktyczne działania dają szansę na realną zmianę sytuacji.

Jakub Syta - dyrektor departamentu cyberbezpieczeństwa w Exatelu

Uporządkowanie odpowiedzialności podmiotów za kwestie bezpieczeństwa cyberprzestrzeni Polski to temat dyskutowany od wielu lat. Wszyscy eksperci jak mantrę powtarzają, że współpraca jest kluczem do skutecznego nadzoru i przeciwdziałania cyberzagrożeniom. Ustawa w zdecydowany sposób tę współpracę ułatwi. Dobrze więc, że prace nad nią udało się sfinalizować. Podmioty, które odrobiły pracę domową i są już technicznie przygotowane do aktywnej ochrony, nie odczują gwałtownych skutków jej wprowadzenia. Pozostałe w szybkim tempie będą musiały nauczyć się, co to znaczy skutecznie chronić systemy teleinformatyczne. Mogę też podkreślić jako praktyk – tego typu wiedza i umiejętności są dziś niezbędne.

Jednak wiele lat pracy nad strategią i samą ustawą sprawiło, że niektóre z zapisów są trudne do zrealizowania. Ciężko sobie choćby wyobrazić, że wszystkie ministerstwa, które dzięki ustawie mogą powoływać własne zespoły reagowania na incydenty teleinformatyczne, będą w stanie to zrobić. Szczególnie, jeśli spojrzymy na liczbę dostępnych na rynku ekspertów oraz konkurencję ze strony międzynarodowych korporacji.