PIĘĆ KLUCZOWYCH WYZWAŃ PRZY WDROŻENIU USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

13.07.2018

Najprawdopodobniej nowy rok szkolny zaczniemy z Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UoKSC). Obecnie jest ona na ostatniej prostej parlamentarnej ścieżki legislacyjnej
(patrz: http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?id=051C4BF2D5C5E6B9C1258287003DC199 **). Lada chwila ta ścieżka zostanie zakończona. Pozostanie podpis prezydenta i odczekanie 14 dni po ogłoszeniu w Dzienniku Ustaw. Jest bardzo prawdopodobne, że 1 września UoKSC będzie już obowiązywała.**

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.

Co powinno podlegać szczególnej weryfikacji w pierwszym okresie funkcjonowania ustawy? Jest moim zdaniem kilka krytycznych wyzwań.

WSPÓŁPRACA CSIRT-ÓW POZIOMU KRAJOWEGO

- poprawne wyznaczenie obszarów odpowiedzialności (constituency);
- transfer wiedzy do najbardziej potrzebujących sektorów;
- wspólne wypracowanie najlepszych praktyki.

Są to wyzwania krytyczne, ale nie negatywne czy pesymistyczne. Przykładem są zadania stawiane przed CSIRT-ami poziomu krajowego, określanymi w ustawie jako CSIRT MON, CSIRT NASK i CSIRT GOV. Jak wiadomo są nimi odpowiednio zespoły CERT-MIL, CERT Polska i CERT.GOV.PL. To na nich spocznie w praktyce odpowiedzialność za to czy będziemy mieli za jakiś czas sprawny system cyberbezpieczeństwa Państwa. Przypisane jest im najwięcej zadań. Powinny dostać mocne wsparcie od wszystkich decydentów. Same jednak staną przed najtrudniejszymi zadaniami. Pierwszym z nich jest poprawne określenie obszarów swojej odpowiedzialności. Jest to dokładnie opisane w Rozdziale 6 Ustawy, ale w praktyce może się okazać, że nie jest to takie proste. Podział wydaje się prosty. W dużym skrócie wygląda on tak – CSIRT MON – obszar wojskowy, CSIRT NASK – obszar cywilny, CSIRT GOV – obszar administracji publicznej. Jeśli jednak zrobimy na to nakładkę takich aspektów jak infrastruktura krytyczna zdefiniowana w ustawie o zarządzaniu kryzysowym, czy działania terrorystyczne, o których mowa ustawie antyterrorystycznej i ustawie o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, to sytuacja się komplikuje. O stanach nadzwyczajnych już nie wspomnę. Decyzja o tym, kto jest głównym odpowiedzialnym za obsługę incydentu i jaka jest rola pozostałych, może nie być prosta. CSIRT-y poziomu krajowego, obok kilku zespołów bezpieczeństwa w największych bankach, telekomach, firmach energetycznych, czy firmach komercyjnych, są najmocniejszymi ośrodkami kompetencji w Polsce w dziedzinie cyberbezpieczeństwa. Na nich głównie spocznie odpowiedzialność praktycznego budowania systemu „w dół" – w poszczególnych sektorach i pod-sektorach wskazanych w załączniku nr 1 do ustawy. W szczególności do tych najbardziej potrzebujących, o których piszę w jednym z następnych punktów. U nich występuje największy deficyt kompetencji. W połączeniu z istotnością systemów obsługiwanych w tych sektorach, tworzy to olbrzymie ryzyko i najsłabsze ogniwa w łańcuchu. CSIRT-y krajowe współpracują ze sobą od lat. Zresztą część ustawy jest wynikiem tej współpracy. Przedstawiciele wszystkich tych zespołów brali czynny udział w pracach nad Ustawą. Teraz na stole leżą konkretne zadania. Trzeba je zamienić w operacyjne zasady współpracy. Kluczowe będzie, aby od początku robić to wspólnie. Zarówno w odniesieniu do współpracy między sobą jaki i z pozostałymi uczestnikami systemu, np: sektorowymi zespołami cyberbezpieczeństwa, a na pewnym etapie również z podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa.

ORGANIZACJA SYSTEMU W POSZCZEGÓLNYCH SEKTORACH

- wykorzystanie wiedzy dojrzałych organizacji;
- poprawne zorganizowanie pracy w organach właściwych.

Ustawa wymienia 6 sektorów operatorów usług kluczowych, 11 podsektorów i 3 usługi definiujące dostawców usług kluczowych. W praktyce wszystkie istotne podmioty pojawiają się w ustawie. Wyjątkiem są firmy telekomunikacyjne, które kierują się Prawem Telekomunikacyjnym, a łączność z częścią zapisów ustawowych, w tym kluczowym zgłaszaniem incydentów, zapewnia w Ustawie pozycja Urzędu Komunikacji Elektronicznej. Poziom dojrzałości „systemu cyberbezpieczeństwa" w tych sektorach jest bardzo różny. Najwięcej doświadczeń posiadają sektor bankowości i finansów, sektor telekomunikacyjny, czy podmioty świadczące usługi cyfrowe. Firmy w tych sektorach od wielu lat rozwijają swoje kompetencje. Są takie sektory jak np. energetyka

(przynajmniej część sektora), które w ostatnich latach mocno przyśpieszyły. Są jednak i takie, o których niewiele możemy powiedzieć. Niestety tę niewiedzę w praktyce musimy zdefiniować jako niski poziom organizacji systemu cyberbezpieczeństwa. Wzrok kieruję na sektor ochrony zdrowia, transportu czy zaopatrzenia w wodę pitną. Organy właściwe dla tych sektorów będą miały pełne ręce roboty. Problem polega na tym, że jak do tej pory te organy, czyli ministerstwa odpowiedzialne za wymienione obszary, nie wykazywały aktywności w zajmowaniu się tematyką cyberbezpieczeństwa. Naiwnością byłoby przypuszczać, że to się nagle zmieni. Oczywiście deklaracje padną, ale cudów nie ma. Trzeba najszybciej zorganizować wsparcie dla tych podmiotów. Każdy będzie mógł się wykazać. Jednak szczególna rola przypada tutaj wspomnianym już CSIRT-om krajowym. Właśnie w tych sektorach w największym stopniu przydałby się program organizacji sektorowych zespołów cyberbezpieczeństwa, które pomogą podmiotom w sektorze. Liczenie na to, że systemem obowiązków i kar doprowadzimy do stworzenia CSIRT-ów np: w szpitalach, to nie tylko naiwność, ale po prostu świadome zaniedbanie.

ZAPANOWANIE NAD TERMINOLOGIĄ I DEFINICJAMI

- zapanowanie nad kategoriami incydentów;
- zorganizowanie systemu praktycznej pomocy przy incydentach.

Konia z rzędem temu kto po przeczytaniu nawet dwu czy trzykrotnym Ustawy z głowy powie czym jest incydent krytyczny, poważny, istotny i (o zgrozo!) incydent w podmiocie publicznym. Samej definicji można się nauczyć. Natomiast zapanowanie nad tym jak każdy z takich incydentów ma być obsłużony? Który zgłaszać i gdzie? Co po zgłoszeniu robić i jak? Obawiam się, że w tym obszarze czeka nas prawdziwa gehenna. Na niespójną terminologię w cyberbezpieczeństwie, poczynając od samego terminu „cyberbezpieczeństwo", narzekają prawie wszyscy. Wiara w idealne rozwiązanie kruszy się. Warto tego problemu nie pogłębiać. System klasyfikacji incydentów nie wygląda dobrze. Chyba tylko wiele godzin ustaleń, może wspólnych warsztatów zainteresowanych podmiotów i konsekwentne stosowanie się przyjętych zasad, może być tu jakimś rozwiązaniem. Na rozporządzenia w tej dziedzinie bym nie liczył. Chyba, że tę kwestię chcemy ograniczyć do półbiurokratycznego działania, związanego z wymogami Ustawy. Jeśli jednak założyć optymistyczny scenariusz, to poprawnie prowadzone klasyfikacje mogą być ważnym elementem obsługi incydentów. Poprawnej klasyfikacji może towarzyszyć jasność co do sposobu działania i zadań poszczególnych organizacji w systemie reagowania.

PRAKTYCZNA ORGANIZACJA KOORDYNACJI KRAJOWEJ

- zdefiniowanie ról zarządczych najwyższego szczebla;
- ćwiczenie sytuacji kryzysowych i funkcjonowania systemu.

W ustawie znajdziemy kilka podmiotów, które aspirują do funkcji koordynacyjnych dla całego systemu cyberbezpieczeństwa Państwa. Niewątpliwe najważniejszym z nich jest funkcja Pełnomocnika rządu do spraw cyberbezpieczeństwa. Nie sposób jednak pominąć przy tej okazji zadań postawionych ministrowi właściwemu do spraw informatyzacji, czyli na dzień dzisiejszy ministrowi cyfryzacji, roli Kolegium przy Radzie Ministrów, czy wreszcie wiodącej funkcji Rządowego Centrum Bezpieczeństwa w działaniach bardzo ważnego zespołu do spraw incydentów krytycznych. W większości przypadków zadania tych podmiotów są dość jasno określone. Jednak nie zawsze i takim przykładem są sprawy międzynarodowe:

„Do zadań Pełnomocnika wykonywanych w porozumieniu z właściwymi ministrami należy również:1) współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi;"

Do zadań ministra właściwego do spraw informatyzacji należy: „koordynacja współpracy między organami właściwymi do spraw cyberbezpieczeństwa i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;"

Trudno przypuszczać, że minister właściwy do spraw informatyzacji będzie koordynował działanie Pełnomocnika. Tego typu nieścisłości warto szybko doprecyzować poprzez robocze ustalenia.

Szczególnie w sytuacjach kryzysowych niejasność kompetencji wielu podmiotów może być groźna. Dlatego trzeba w krótkim czasie sprawić, aby w warunkach „pokojowych" te wątpliwości rozwiać i ustalić jak koordynacja wygląda w praktyce. Najlepszym narzędziem do tego będzie organizacja ćwiczeń. Inicjowanie krajowych ćwiczeń w zakresie cyberbezpieczeństwa jest na wprost wpisane w zadaniach Pełnomocnika. Przynajmniej tutaj sytuację mamy jasną. Warto takie ćwiczenia przeprowadzić stosunkowo szybko. Powinny to być ćwiczenia o charakterze strategicznym. Odpowiednio przygotowany scenariusz będzie w stanie uwzględnić wszystkie potencjalnie niejasne sytuacje, a analiza przebiegu ćwiczeń będzie najlepszym materiałem wskazującym optymalny model systemu.

BUDŻET

Trudno tu wymieniać punkty wskazujące najważniejsze działania. Budżet najzwyklej w świecie musi być znacznie większy. Szczęśliwie skończyliśmy z kuriozum z „Polityki Ochrony Cyberprzestrzeni RP" jakim był zapis, że jej wdrożenie nie wymaga środków budżetowych. Nie znaczy jednak, że jest dobrze. Kwota około 90 mln złotych, którą można zliczyć w art. 93 Ustawy jest oczywiście kroplą w morzu potrzeb, szczególnie jeśli dotyczy okresu dziesięcioletniego. Na szczęście to nie są całkowite środki. Przede wszystkim jak łatwo zauważyć, w Ustawie nie pojawia się budżet dla MON. Oznacza to, że MON pokryje swoje wydatki z już istniejącego budżetu i być może będą to środki największe w całym systemie. Pozostają jeszcze działania związane z pozyskiwaniem grantów. Nie zmienia to faktu, że konieczne jest aby w przyszłych budżetach Państwa pojawiły się pozycje dotyczące wydatków na cyberbezpieczeństwo. Pamiętajmy o wielkiej pracy do wykonania w wielu zaniedbanych sektorach, które wg art. 93 otrzymują niezwykle ograniczone środki. Pewnym ratunkiem jest fakt, że gro wydatków pójdzie z kieszeni podmiotów prywatnych, działających w sektorach objętych Ustawą. To zresztą nic nowego. Banki, telekomy, czy operatorzy infrastruktury krytycznej od lat wydają duże środki na ten cel.

JAK WIĘC BĘDZIE?

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.

Autor:
Mirosław Maj – Prezes Fundacji Bezpieczna Cyberprzestrzeń

Śledź nas na:
TT: @cybsecurity_org
Facebook: **@FundacjaBezpiecznaCyberprzestrzen**