Rekomendacje

Zarządu Stowarzyszenia Euro-Atlantyckiego

w sprawie wprowadzenia stanu nadzwyczajnego w związku z zagrożeniami z cyberprzestrzeni

Latem ubiegłego roku uchwalono nowelizację ustaw o stanach nadzwyczajnych, według projektu wniesionego do Sejmu z inicjatywy Prezydenta. Ważną systemową zmianą w sprawie przesłanek dla wprowadzania stanów nadzwyczajnych określonych art. 228 Konstytucji Rzeczypospolitej Polskiej, jest uwzględnienie potencjalnych zagrożeń dla państwa, wynikających z działań w cyberprzestrzeni. Wprowadzenie przez Prezydenta RP stanu wyjątkowego, stanu klęski żywiołowej, a tym bardziej znalezienie się Polski w stanie wojny to sytuacje bardzo szczególne. Zawiesza się wtedy niektóre gwarantowane Konstytucją prawa obywatelskie i niektóre zwykłe procedury administracyjne, służby państwowe uzyskują dodatkowe uprawnienia, podmioty gospodarcze mogą być poddane nietypowym rygorom, a dysponenci infrastruktury wykonujący zadania użyteczności publicznej mogą zostać zmobilizowani do dodatkowych świadczeń, a nawet zmilitaryzowani.

Wprowadzenie stanu nadzwyczajnego musi się opierać o twarde, weryfikowalne przesłanki. Znalezienie dla nich uzasadnienia w zagrożeniach z cyberprzestrzeni jest złożonym zagadnieniem, bo w dużej części tego rodzaju zagrożenia dla funkcjonowania państwa mają dzisiaj charakter potencjalny lub ograniczają się do działań lub zdarzeń, które z punktu widzenia bezpieczeństwa lub obronności państwa należy kwalifikować jako incydenty, nawet jeżeli w przekazie medialnym wyglądają na spektakularne lub rozległe. Przygotowanie do nich wymaga podejmowania przez państwo systemowych działań zaradczych w dziedzinie bezpieczeństwa informacyjnego, uwzględniających rosnące wielosektorowe i wieloaspektowe znaczenie technologii informacyjnych, nowych usług i aplikacji. Wiadomo też, że trzeba organizować dynamicznie

nowoczesne sposoby ochrony systemów informacyjnych, klasyfikacji informacji, wdrażać stosowne środki techniczne, standardy, procedury.

Trzeba podnosić zdolności analizowania zagrożeń, zapewniając warunki dla skutecznego reagowania dysponentom infrastruktury krytycznej, organom władzy publicznej oraz instytucjom państwa właściwym w sprawach bezpieczeństwa i obronności państwa oraz bezpieczeństwa i porządku publicznego. Wprowadzenie stanu nadzwyczajnego może się stać uzasadnione, podobnie jak w przypadku innego rodzaju zagrożeń, dopiero wtedy kiedy zwykłe środki prawne na pewno nie będą wystarczające do skutecznego zarządzania sytuacją kryzysową.

Trzeba też zwrócić uwagę, że w obowiązującym stanie prawnym w Prawie telekomunikacyjnym są przepisy nakładające na przedsiębiorców telekomunikacyjnych obowiązki w związku z bezpieczeństwem sieci i usług telekomunikacyjnych oraz ciągłością świadczenia usług (art.178 ust.3 Prawa telekomunikacyjnego).

Operatorzy są na przykład zobowiązani do posiadania planów działań w sytuacjach szczególnych zagrożeń, uzgadnianych ze stosownymi organami administracji rządowej i samorządowej. Ustawa pozwala ponadto nakładać na operatorów telekomunikacyjnych obowiązki związane z ograniczeniem łączności na określonym obszarze, co może być zastosowane np. w związku z zagrożeniem terrorystycznym. Przedsiębiorcy telekomunikacyjni są zobowiązani do podejmowania działań zaradczych, zapewniających ciągłość świadczenia usług, odtwarzanie utraconych, uszkodzonych lub zablokowanych zasobów, utrzymanie bezpieczeństwa i zachowanie tajemnicy telekomunikacyjnej. W zakresie określonym stosownymi przepisami ustawy powinni zachować zdolność współpracy ze służbami właściwymi w sprawach bezpieczeństwa i obronności państwa oraz bezpieczeństwa i porządku publicznego.

WPROWADZENIE STANÓW NADZWYCZAJNYCH – PRZYKŁADOWE PRZESŁANKI

Zmasowane cyberataki – są najbardziej oczywistym powodem zagrożenia państwa z wykorzystaniem technologii informacyjnych. Należy się liczyć z tym, że tego różnego rodzaju techniki ataków zostałyby zastosowane jako środek odstraszania lub wsparcie konwencjonalnych ataków militarnych w działaniach wojennych, również niekoniecznie bezpośrednio

w związku z wojną na terytorium Polski, ale jako uboczny efekt wojny wobec któregoś z sojuszników.

Skuteczny atak na systemy infrastruktury krytycznej, zablokowanie, uszkodzenie, spowodowanie wadliwego działania lub przejecie kontroli może uniemożliwić normalne funkcjonowanie państwa. Może to być efekt fiaska działań dyplomatycznych w negocjacjach z wrogim państwem. Taki atak może być użyty jako środek nacisku, wykazanie przewagi technologicznej bez użycia konwencjonalnych środków militarnych. Celowe ataki byłyby też z pewnością użyte, jako część działań wspierających akcję militarną.

Może to też nastąpić z pobudek terrorystycznych, by skompromitować rząd, licząc na sprowokowanie paniki lub masowego niezadowolenia ze sposobu działania rządzących w sytuacji kryzysowej.

Niektóre systemy infrastruktury krytycznej mają zasięg lub oddziaływanie międzynarodowe. Tego rodzaju atak może mieć motywacje i skutki ekonomiczne, uderzając w międzynarodową wymianę handlową. Zorganizowane działanie może być obliczone na destabilizację sytuacji międzynarodowej, wywołanie konfliktu o zasięgu globalnym.

Zmasowany atak na systemy identyfikacji i uwierzytelniania - kradzież wrażliwych danych osobowych na ogromną skalę, mogłaby być hipotetycznym skutkiem złamania jednego z ważnych powszechnie używanych zabezpieczeń, przykładowo skompromitowania całej kryptografii klucza publicznego. Uniemożliwiłoby to stosowanie wielu systemów płatności elektronicznej, bankowości, rozliczeń w sieciach telekomunikacyjnych.

Zmasowana akcja dezinformacyjna - wrogie zorganizowane działania z użyciem różnych mediów elektronicznych, w tym mediów społecznościowych, jeżeli są starannie wyreżyserowane, a z tym należy się liczyć, mogą być istotnym czynnikiem destabilizującym sytuację w państwie.

Sztormy geomagnetyczne – są spowodowane w ziemskiej atmosferze przez wyjątkowo aktywne Słońce uszkadzając działanie satelitów telekomunikacyjnych, radiowych systemów łączności. W sytuacji skrajnej może to dać powód do ogłoszenia stanu klęski żywiołowej. Słońce w ciągu ostatnich kilkunastu lat było wyjątkowo spokojne, ale teraz wkracza w fazę aktywną.

REKOMENDACJE

1. Autorytet państwa nie powinien być angażowany w klasyfikowanie i uregulowanie wszelkich rodzajów zagrożeń z cyberprzestrzeni. Państwo zapewnia istnienie i funkcjonowanie podstawowych ram prawnych. Państwo może odpowiednią polityką tworzyć warunki dla wzmacniania bezpieczeństwa, pełnić rolę animatora standaryzacji i dobrych praktyk, ale proces legislacyjny jest zbyt wolny, by nadążać za dynamiką pojawiania się nowych typów zagrożeń, związanych z wykorzystywaniem technologii informacyjnych, usług lub aplikacji.

2. Penalizowanie zagrożeń z cyberprzestrzeni powinno się opierać przede wszystkim o sprawdzone klauzule generalne. Tendencja do wygodnego dla wymiaru sprawiedliwości uszczegóławiania norm prawa karnego nie nadąża za inwencją tych, których próbujemy nazywać cyberprzestępcami lub cyberterrorystami.

3. Uregulowanie obowiązków przedsiębiorców telekomunikacyjnych w sytuacjach kryzysowych zagrażających ciągłości świadczenia usług telekomunikacyjnych, opiera się o ustawowy obowiązek posiadania zatwierdzonych w procedurze administracyjnej planów działań w sytuacjach szczególnych zagrożeń (Art. 176a Prawa telekomunikacyjnego). Ten mechanizm nie jest odpowiedni dla zagrożeń z cyberprzestrzeni, ponieważ nie będzie za nimi nadążać. Ustalanie sposobów reagowania na zagrożenia z cyberprzestrzeni powinno być działaniem ciągłym. Pomocne byłoby w tej sytuacji wdrażanie przepisów motywujących funkcjonowanie technicznych grup roboczych, forów wymiany doświadczeń o zagrożeniach. Trzeba przy tym uwzględnić, że zagrożenia z cyberprzestrzeni mogą mieć wpływ na sposób reagowania na podstawie dotychczasowych „tradycyjnych" planów działań.

4. Procedury ustalania obiektów infrastruktury krytycznej, w pod rządami obowiązującej ustawy o zarządzaniu kryzysowym nie będą nadążać za zagrożeniami z cyberprzestrzeni. Wybór obiektów dla najbardziej dotkliwego lub spektakularnego ataku, wykrycie przez atakującego podatności i opracowanie mechanizm ataku nie muszą odpowiadać oszacowaniom z perspektywy organów administracji odpowiedzialnych za planowanie kryzysowe w państwie. Należałoby rekomendować raczej zastosowanie podejścia sektorowego,

w którym sami posiadacze różnego rodzaju infrastruktury, szczególnie z sektora prywatnego, zostaliby zmotywowani do gromadzenia i wymiany doświadczeń w kwestiach bezpieczeństwa, a także analizowania korelacji mogących wpływać na bezpieczeństwo zarządzanej infrastruktury i obsługujących ją systemów teleinformatycznych.

5. Ograniczanie lub blokowanie dostępności usług zarządzane w sytuacjach wystąpienia szczególnego zagrożenia2 musi uwzględniać coraz większe znaczenie komunikacji dla innych użytkowników, konsumentów, systemów zdalnego sterowania sieciami urządzeń. Trzeba się liczyć z tym, że będzie to coraz trudniej akceptowane przez użytkowników, a w przypadkach prawdziwych zagrożeń może się przyczyniać do wtórnego pogłębiania skutków kryzysu. Należałoby wprowadzić zasady stosowania tego typy ograniczeń, tak by ustawowa przesłanka wskazana w ust. 1 art. 178 *„kierowania się rozmiarem zagrożenia i potrzebą ograniczenia jego skutków, z zachowaniem zasady minimalizowania negatywnych skutków nałożonych obowiązków dla ciągłości świadczenia usług i działalności gospodarczej przedsiębiorcy”* była zrozumiała i akceptowana zarówno przez przedsiębiorców telekomunikacyjnych, jak i użytkowników usług. To samo dotyczy stosowania przez upoważnione organy urządzeń uniemożliwiających telekomunikację, działających na podstawie upoważnienia art. 178 ust.3, którym nie wskazano w ustawie żadnych przesłanek dla tego rodzaju działań.

6. Reagowanie w stanach nadzwyczajnych – może uzasadnić użycie środków, naruszających prywatność, prawa własności intelektualnej, bezpieczeństwo obrotu gospodarczego, ujawnienie zbiorów danych osobowych. Wzrost znaczenia technologii informacyjnych spotęguje ryzyko tego rodzaju naruszeń. Należy te kwestie rozstrzygnąć pod kątem prawnym, a także wprowadzić procedury niwelowania negatywnych skutków naruszenia cyberbezpieczeństwa osób prywatnych i podmiotów gospodarczych w następstwie wprowadzenia stanu nadzwyczajnego.

Stowarzyszenie Euro-Atlantyckie i Fundacja „Instytut Mikromakro” deklarują gotowość współdziałania z osobami i instytucjami odpowiedzialnymi za obronę przed zagrożeniami z cyberprzestrzeni.