Cyber Security 2013 – wnioski dla Polski

#Strategia i polityka 29 października 2013

Wczoraj w Warszawie odbyła się Międzynarodowa Konferencja i Wystawa Cyber Security 2013. Tematem przewodnim imprezy były *Zagrożenia w cyberprzestrzeni – bezpieczeństwo ponad granicami*.

Tegoroczna konferencja dowiodła, że kwestia cyberbezpieczeństwa jest coraz bardziej doceniana przez przedstawicieli przemysłu, a także administracji państwowej

Impreza, której organizatorami byli Zarząd Targów Warszawskich S.A. (ZTW) i Agencja Lotnicza ALTAIR, zgromadziła liczne grono najwybitniejszych specjalistów z Polski i świata, zajmujących się problematyką cyberbezpieczeństwa. Warto wspomnieć, że jest ona kontynuacją Międzynarodowej Konferencji i Wystawy Cło i Granica (Bezpieczeństwo państwa przede wszystkim, 2012-11-22), przeniesionej w nowy wymiar zapewnienia bezpieczeństwa Państwa, Obywateli i kluczowej infrastruktury.

Po powitaniu zgromadzonych gości przez p. Grażynę Karłowską, wiceprezes Zarządu ZTW i Wojciecha Łuczaka, wiceprezesa ds. wydawniczych AL ALTAIR, moderator gen. bryg. (rez.) Adam Sowa rozpoczął dyskusję w ramach pierwszego panelu, zatytułowanego *Cyberzagrożenia i sposoby przeciwdziałania tym zjawiskom w odniesieniu do administracji publicznej, obronności i bezpieczeństwa państwa oraz ochrony porządku publicznego*. Gen. Sowa zwrócił uwagę, że cyberprzestrzeń stała się już domeną operacyjną i nazywana jest *piątym wymiarem działania*. W ramach Sił Zbrojnych USA już od 2006 funkcjonuje już Cyber Command, którego zadaniem jest prowadzenie operacji w cyberprzestrzeni, mających na celu ochronę krytycznej infrastruktury Stanów Zjednoczonych przed atakami hakerskimi, wsparcie poszczególnych rodzajów sił zbrojnych oraz ochronę infrastruktury informacyjnej Departamentu Obrony.

Z kolei gen. Krzysztof Bondaryk, Dyrektor Narodowego Centrum Kryptologii, zwrócił uwagę, że obecnie świat realny i wirtualny przenikają się coraz bardziej. *Cyberprzestępczość nie zna granic, dlatego konieczna jest współpraca międzynarodowa i budowanie narodowych zdolności do obrony przed atakiem cybernetycznym. Niestety, przeszkadzają w tym problemy kulturowe, mentalne, a przede wszystkim techniczne. W dodatku świat wirtualny jest odległy od polityki. Powoduje to, że w naszym kraju brak jest wizji cyberbezpieczeństwa. Dopiero po 5 latach dyskusji, w czerwcu br. podjęto pierwszą próbę sformułowania polityki ochrony w tej dziedzinie. Inne kraje ustaliły to już dekadę wcześniej, a teraz realizują kwestie techniczne* – stwierdził gen. Bondaryk.

W Polsce jednym z największych problemów jest brak kultury korporacyjnej ochrony informacji i mieszanie priorytetów. Brak jest dobrego przykładu, idącego *z góry*, a zarządzenia są ignorowane w praktyce. Często brak jest odpowiednich środków na bezpieczeństwo cybernetyczne lub są one zbyt małe. Człowiek wciąż pozostaje najsłabszym elementem ochrony, dlatego trzeba zwiększać świadomość obywateli, co do zagrożeń związanych z komputeryzacją. Bez cyberbezpieczeństwa nie ma bezpieczeństwa Polski – podsumował Dyrektor Narodowego Centrum Kryptologii.

Powitanie zgromadzonych gości przez p. Grażynę Karłowską, wiceprezes Zarządu ZTW i Wojciecha Łuczaka, wiceprezesa ds. wydawniczych AL ALTAIR

Myśl tę rozwinęła Henryka Bochniarz, wiceprezes Boeinga na Europę Środkową i Wschodnią, mówiąc, iż *komputery są nieodłącznym elementem naszego życia i już od najmłodszych lat trzeba budować świadomość bezpieczeństwa cybernetycznego*. *Przeciętny użytkownik wie niewiele na temat cyberprzestrzeni. Haker porusza się w niej bez problemów.* Według informacji przedstawionych przez p. Bochniarz codziennie ofiarą ataków hakerskich pada 1 milion osób. Przestępstwa tego typu powodują roczne straty w wysokości 300 mln euro. Każdego tygodnia wykonywanych jest 2 mln ataków na przedsiębiorstwa, z czego 70% ma na celu zdobycie danych. *W celu ochrony przed takimi incydentami konieczne jest uwzględnienie potrzeb już na etapie projektowania.*

Niezbędna jest współpraca publiczno-prywatna i jednakowy dla wszystkich użytkowników system ochrony. Pamiętajmy, że bezpieczeństwo sieci to tylko środek, a nie cel sam w sobie – podkreśliła Henryka Bochniarz.

Kolejny mówca, płk Kazimierz Mordaszewski, reprezentujący *Rządowy Zespół Reagowania na Incydenty Komputerowe*(CERT) przedstawił sytuację dotyczącą cyberprzestępczości w Polsce. Przypomniał, że skutki włamań hakerów mogą być bardzo daleko idące, a wszystkie tego typu incydenty należy zgłaszać w celu wyciągnięcia z nich wniosków na przyszłość.

Nieco bardziej optymistyczną wizję wirtualnej rzeczywistości zaprezentowali p. Agata Szydełko i Frederic Jordan z Agencji ds. Łączności i Informacji NATO. Sojusz wdraża obecnie strategię *Smart Defence*, której podstawowym celem jest wspólne opracowanie, pozyskanie i utrzymywanie zdolności do prowadzenia działań w cyberprzestrzeni, uznanej za *nowy wymiar przestrzeni bitewnej*. *Smart Defence* polega na rozwoju narodowych zdolności w zakresie cyberbezpieczeństwa i współdzieleniu ich z innymi krajami. *Dzielenie się jest ważniejsze niż strach przed podzieleniem się informacją* – zauważyła Agata Szydełko. *Wszystkie kraje są w podobnej sytuacji. NATO robi wiele, ale sieci krajowe są poza siecią NATO. Dlatego konieczna jest interoperacyjność* – dodał Frederic Jordan. Na razie w przedsięwzięciu bierze udział tylko 5 krajów: Kanada (państwo wiodące), Dania, Holandia, Norwegia i Rumunia, jednak przystąpić mogą do niego wszyscy zainteresowani – zarówno członkowie NATO, jak i kraje partnerskie. Budżet inicjatywy wynosi 60 mln euro, a zgłoszenie całkowitej zdolności operacyjnej nastąpić ma za 2 lata.

W dalszej części dyskusji Dewey Houck, z Boeing Electronic & Information Solutions przypomniał, że na świecie jest coraz więcej urządzeń mających dostęp do Internetu. Za kilka lat ich liczba sięgnie 30 miliardów. Dlatego też konieczne jest współdziałanie NATO i USA w zakresie cyberbezpieczeństwa i wypracowanie wspólnych procedur.

Dr Krzysztof Liedel, przedstawiciel Biura Bezpieczeństwa Narodowego poinformował, że MON opracowuje nową strategię działania, której część została poświęcona zagadnieniom bezpieczeństwa cybernetycznego. *Nie da się zabezpieczyć całej cyberprzestrzeni. Należy zatem chronić krytyczną strukturę teleinformatyczną państwa* – stwierdził dr Liedel. W tym celu konieczne jest wypracowanie spójnej polityki państwa w tym zakresie, niestety, jak już wspomniano na wstępie, brak jest w Polsce specjalistów w tej dziedzinie.

Piotr Ciepiela z Ernst & Young, zajmujący się bezpieczeństwem infrastruktury krytycznej zwrócił uwagę na obszar Bliskiego Wschodu, będący od 3 lat polem cyberbitew pomiędzy terrorystami, stosującymi coraz bardziej wyrafinowane i skuteczne sposoby, a specjalistami odpowiedzialnymi za bezpieczeństwo. Co najgorsze

dla użytkowników sieci komputerowych, narzędzia do prowadzenia cyberwalki są powszechnie dostępne w Internecie. *Dziś nie potrzeba już specjalistycznej wiedzy, aby przeprowadzić cyberatak. Może to zrobić nieświadomie nawet 10-latek* – stwierdził Piotr Ciepiela. Trzeba zatem myśleć o edukacji od podstaw społeczeństwa komputerowego, jakim de facto jesteśmy i zabezpieczeniach sieci komputerowej przed dostępem dzieci i osób niepowołanych.

Podobne koncepcje promował Adam Bartosiewicz, Wiceprezes Zarządu ds. Rozwoju przedsiębiorstwa WB Electronics, który zauważył, że *cyberprzestrzeń zapewnia przewagę w realnym życiu, dlatego obydwie dziedziny należy rozpatrywać kompleksowo. Pojedynczy pendrive ma dziś siłę rażenia większą niż dywizja wojska.* W dalszej części swojego wystąpienia prezes Bartosiewicz zaskoczył nieco zebranych, mówiąc, że Polska postrzegana jest w świecie jako kraj mający duże kompetencje w dziedzinie bezpieczeństwa cybernetycznego. *Ponieważ jesteśmy państwem średniej wielkości, bez ambicji mocarstwowych, możemy dzięki temu stać się bezpiecznym dostawcą technologii komputerowych dla innych krajów* – stwierdził prezes Bartosiewicz. Niestety, najtrudniej być prorokiem we własnym kraju. Według Adama Bartosiewicza oparcie polskiej sieci telekomunikacyjnej na rozwiązaniach obcych, nad którymi nie ma żadnej kontroli, powoduje, że są one narażone na nieuprawniony podsłuch lub zdalne wyłączenie części lub wszystkich usług. Rozwiązaniem problemu może być wdrożenie nowej sieci (NYX), zapewniającej bezpieczeństwo, anonimowość i odporność na ataki.

Dr hab. inż. Zbigniew Tarapata, Dyrektor Instytutu Systemów Informatycznych Wydziału Cybernetyki Wojskowej Akademii Technicznej zauważył, że uczelnia, jako druga w Europie, rozpoczęła już kształcenie specjalistów w dziedzinie kryptologii, a w najbliższych latach ich liczba ma wzrosnąć. Odbudowanie polskiej szkoły kryptologii pozwoli na odzyskanie jurysdykcji nad systemami teleinformatycznymi.

Konferencji towarzyszyła wystawa przedsiębiorstw oferujących usługi i rozwiązania związane z działaniami w cyberprzestrzeni / Zdjęcia: Bartosz Głowacki

Jak wiadomo, obecnie trwa organizowanie Narodowego Centrum Kryptologii. W prace zaangażowane są MON, ABW i WAT. Gen. Bondaryk, indagowany w tej kwestii przez uczestników konferencji poinformował ich, *ze cele strategiczne NCK zostaną zrealizowane w ciągu 5 lat*. Więcej szczegółów gen. Bondaryk nie ujawnił, zasłaniając się tajemnicą państwową. Odpowiadając na pytanie przedstawiciela Boeinga, jakie rozwiązanie zadowoli polski rząd odparł, że *musi być ono dobre, bezpieczne i tanie. Musi to być rozwiązanie narodowe lub odpowiednio zmodyfikowana adaptacja technologii obcych, z zachowaniem prawa własności*. *Oprócz tego Polsce potrzeba nowych specjalistów od bezpieczeństwa sieciowego i używania systemów bezpieczeństwa* – podsumował gen. Bondaryk.

Podczas dyskusji na zakończenie panelu dr Liedel przyznał także, iż nie ma w Polsce szczegółowych dokumentów regulujących kwestie cyberbezpieczeństwa. *Są rozwiązania przejściowe, trzeba wypracować strategię. Brak jest także instytucji koordynującej takie działania, ale może to być równie dobrze mechanizm. Obecnie kwestiami cyberbezpieczeństwa zajmuje się Ministerstwo Administracji i Cyfryzacji* – stwierdził dr Liedel.

Konrad Gałczyński, reprezentujący Ministerstwo Spraw Zagranicznych, przedstawił pogląd NATO na cyberatak, według którego *niczym nie różni się on od klasycznego ataku zbrojnego*. Mimo tego sojusznicy nie mają obowiązku pomagać sobie w razie ataku cybernetycznego. Sojusz jedynie może apelować o wolę polityczną do współpracy przy problemie cyberbezpieczeństwa. *Brak jest aktów prawnych dotyczących wojny w cyberprzestrzeni. Wiemy tylko, że zespoły narodowe bronią zasobów wewnętrznych i nie wpuszczamy obcych do swojej sieci komputerowej* – dodałKonrad Gałczyński.

Powiązane wiadomości

Cyber Security 2013 – wnioski dla Polski (2013-10-29)
- Bezpieczeństwo państwa przede wszystkim (2012-11-22)
  - Informacja najważniejszym orężem bezpieczeństwa (2011-11-11)
  - Polskie lotniska gotowe na Euro 2012 (2012-03-27)
  - Przyszłość bezzałogowców dla WP (2012-04-05)
    - Taktyczne bsl – więcej szczegółów (2010-02-01)
    - Seryjne FlyEye dostarczone (2010-12-11)
  - MON stawia na bezzałogowce (2012-07-22)
  - 2 mld GBP na brytyjskie bezzałogowce (2012-09-29)
    - Kolejnych 40 mln GBP na Taranisa (2011-12-25)
    - Porozumienie w sprawie rozwoju bsl (2012-07-26)
  - 7500 amerykańskich bsl (2012-11-05)
    - RQ-170 w rękach Iranu (2011-12-09)
    - Iran buduje kopię RQ-170 (2012-04-22)