DGP ekstra

BEZPIECZEŃSTWO INFORMATYCZNE

Wtorek 8 stycznia 2013, nr 5 (3395) gazetaprawna.pl

Systemy informatyczne państwa wymagają szczególnego nadzoru

Państwo powinno zadbać o solidne zabezpieczenie krytycznych dla jego funkcjonowania systemów. Lista instytucji, które powinny **stawiać na jakość**, a nie najniższą cenę, jest długa

W Polsce wiele istotnych dla funkcjonowania państwa systemów obsługiwanych jest przez firmy, które wystartowały w otwartych przetargach publicznych i wygrały je. Zdarza się, że nawet przy realizacji najważniejszych projektów w policji, sądownictwie czy administracji przetwarzającej wrażliwe dane dotyczące niemal wszystkich obywateli nie stosuje się żadnej ochrony – brak barier przed firmami potencjalnie nieuczciwymi czy niosącymi zagrożenia dla bezpieczeństwa. W takich przypadkach żądania dostarczenia dokumentów o niekaralności członków zarządu i niezaleganiu ze składkami są na pewno niewystarczającymi środkami bezpieczeństwa. Bo też zagrożenia są realne – należy ocenić ryzyko, jakie z nich wynika i dobrać odpowiednie zabezpieczenia.

Do dyskusji o strategii rozwoju systemu bezpieczeństwa narodowego warto dołączyć temat kluczowych dla funkcjonowania państwa polskiego rozwiązań IT.

Systemy szczególnej ochrony

Jednym z najważniejszych systemów, w których dane muszą być chronione w sposób szczególny, jest Kompleksowy System Informatyczny Zakładu Ubezpieczeń Społecznych, w którym przetwarzane są wrażliwe dane prawie wszystkich obywateli. Podobnie jest w przypadku aplikacji dla sektora zdrowia utrzymywanych przez Narodowy Fundusz Zdrowia oraz jego ośrodki czy budowanej przez Centrum Systemów Informacyjnych Ochrony Zdrowia (jednostkę podległą Ministerstwu Zdrowia) elektronicznej platformy gromadzenia, analizy i udostępniania zasobów cyfrowych o Zdarzeniach Medycznych (tzw. Projekt P1) oraz systemów jej towarzyszących (platforma udostępniania online przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych, elektroniczna platforma konsultacyjnych usług telemedycznych Ministerstwa Zdrowia, NFZ oraz sieci szpitali wysokospecjalistycznych, e-recepta czy internetowe konto pacjenta).

Równie istotne dane, które powinny być jak najlepiej chronione przed szpiegostwem i potencjalnymi działaniami terrorystycznymi, przetwarzają systemy Ministerstwa Spraw Wewnętrznych oraz Ministerstwa Administracji i Cyfryzacji, CEPiK (Centralna Ewidencja Pojazdów i Kierowców), PESEL (Powszechny Elektroniczny System Ewidencji Ludności), na którego bazie powstaje pl.ID (nowy dowód osobisty), systemy paszportowe, powiadamiania ratunkowego, STAP (Sieć Teleinformatyczna Administracji Publicznej) i inne systemy łączności, czy wreszcie ePUAP (Elektroniczna Platforma Usług Administracji Publicznej). Te rozwiązania na pewno wymagają szczególnej troski i miejsca we wszystkich strategiach dotyczących bezpieczeństwa teleinformatycznego państwa.

Projekty cywilne i mundurowe

Podobnie jest w przypadku projektów teleinformatycznych związanych z sektorem finansowym i zarządzaniem gospodarką. Szczególnego nadzoru wymagają: zintegrowane systemy obsługi budżetu państwa, systemy scentralizowane obsługujące Narodowy Bank Polski, Bank Gospodarstwa Krajowego, PKO BP, PZU, Giełdę Papierów Wartościowych w Warszawie, rozwiązania IT nadzoru finansowego i ubezpieczeniowego, e–podatki, systemy celne czy realizujące dopłaty rolne (w Agencji Restrukturyzacji i Modernizacji Rolnictwa). We wszystkich gałęziach gospodarki uważanych za strategiczne i tam, gdzie przetwarzane są duże ilości danych obywateli (Poczta Polska, energetyka, łączność), nadzór nad systemami IT powinien być skrupulatnie sprawowany, a zawarte w nich dane powinny być zabezpieczone, również przed zagrożeniami wewnętrznymi, a nie tylko zewnętrznymi.

Równie istotne jest zapewnienie odpowiedniego nadzoru nad systemami centralnymi i „cywilnymi" w sektorze mundurowym. Z definicji realizują one zadania z zakresu bezpieczeństwa, w którym praca na danych wrażliwych i dostęp do poufnych informacji są codziennością. Kompleksowy System Informacyjny Policji i inne rozwiązania wykorzystywane przez tę formację, systemy nadzoru granicy i obsługi Straży Granicznej, rozwiązania stosowane przez Państwową Straż Pożarną to projekty, w których poszczególne prace są często zlecane w otwartych przetargach. Co gorsza, zwycięzca nie musi gwarantować najwyższej jakości usług, bo liczy się tylko cena.

Kompleksowy System Informacyjny Policji i inne rozwiązania wykorzystywane przez tę formację, systemy nadzoru granicy i obsługi Straży Granicznej, rozwiązania stosowane przez Państwową Straż Pożarną to projekty, w których poszczególne prace są często zlecane w otwartych przetargach. Co gorsza, zwycięzca nie musi gwarantować najwyższej jakości usług, bo liczy się tylko cena

Niższe koszty ważniejsze od bezpieczeństwa

Dbałość zamawiających o budżet i oszczędne gospodarowanie środkami bywają ważniejsze niż braki w zabezpieczeniach. Niestety chodzi o rozwiązania zasługujące na szczególną uwagę, gdzie szpiegostwo, awarie czy ataki terrorystyczne mogłyby doprowadzić do skutków trudnych do naprawienia.

Podobnie jest w przypadku kluczowych systemów działających w ministerstwach, które realizują zadania ważne dla gospodarki, dyplomacji czy sprawiedliwości. Gdyby Ministerstwo Spraw Zagranicznych padło ofiarą szpiegostwa, kradzieży danych czy cyberataku terrorystycznego, szkody dyplomatyczne i wizerunkowe również byłyby ciężkie do naprawienia. Nie mniej istotne jest bezpieczeństwo systemów i infrastruktury użytkowanych przez organy resortu sprawiedliwości: samego ministerstwa, struktur więziennictwa, prokuratur, sądów, instytucji nadzorujących poszczególne gałęzie gospodarki oraz kontrolujące zagrożenia naturalne (np. IMiGW).

We wszystkich tych miejscach zwiększenie nadzoru nad projektami i zapewnienie ich realizacji przez wiarygodnych partnerów podlegających w pełni polskiemu nadzorowi mają niezwykle istotne znaczenie dla ich bezpieczeństwa oraz dla bezpieczeństwa polskiego państwa.

Cezary Warda

Dane i tajemnice łatwo mogą stać się łupem szpiegów

Co kilka miesięcy wybucha na świecie skandal związany z podejrzeniami o działalność szpiegowską jednego z **dostawców technologii i usług informatycznych**

Wiele rządów wyklucza powierzanie zagranicznym firmom najważniejszych systemów informatycznych, szczególnie tych analizujących dane wrażliwe dla obywateli lub bezpieczeństwa państwa. Jeśli nawet technologie są kupowane od korporacji zagranicznych, to zawsze w takich przypadkach pełną kontrolę nad wdrożeniem sprawuje zaufana firma rodzima. W USA, Wielkiej Brytanii, Francji, Izraelu czy w Niemczech jest nie do pomyślenia, by ważne dla funkcjonowania państwa systemy teleinformatyczne pozostawały pod nadzorem obcych firm. I nikt nie przejmuje się zarzutami o faworyzowanie „swoich", gdy media co chwila donoszą o atakach hakerskich, działaniach szpiegowskich czy cyberwłamaniach.

Szpiedzy i włamywacze

W 2010 roku przedmiotem zainteresowania była korporacja Google, której niemieccy urzędnicy zarzucili łamanie prawa przy zbieraniu danych do map i baz zdjęciowych. Samochody rejestrujące dane na zlecenie Google poza zdjęciami ściągały też dane z niezabezpieczonych sieci bezprzewodowych. Google tłumaczył w „Financial Timesie", że to wina jednego z inżynierów, który wprowadził nieautoryzowany kod do oprogramowania. Potem okazało się, że dane zbierano celowo, ale nie zdając sobie sprawy z możliwości złamania przepisów i bez złej woli.

Szerokim echem odbiła się też afera Nortela, upadłego giganta telekomunikacyjnego, którego przez prawie 10 lat mieli inwigilować i szpiegować hakerzy z Chin. Sprawę ujawnił wewnętrzny audytor, który opowiedział dziennikarzom, że z serwerów firmy kradziono latami dokumentacje, raporty, e-maile i inne dokumenty biznesowe. W procederze wykorzystywano loginy i hasła ukradzione menedżerom Nortela, m.in. samemu prezesowi korporacji.

Dość często pojawia się zarzut, że operatorzy komunikatorów internetowych i portali społecznościowych szpiegują użytkowników. W grudniu 2011 r. podniesiono, że oprogramowanie szpiegujące jest instalowane na milionach smartfonów.

Komu dostęp do danych

Oskarżenia wobec dostawców technologii rzucane są także w Polsce. Szczególnie w przypadkach, w których firmy proponują niskie ceny za usługi lub dostawy. We wrześniu 2011 r. Dziennik Gazeta Prawna poinformował, że Ministerstwo Spraw Wewnętrznych jest sponsorowane przez... Huawei. Resort przyznał, że dostał od tej firmy sprzęt do testów organizacji wideokonferencji.

„(Ministerstwo) nawet nie sprawdziło ich pod kątem bezpieczeństwa – czy na przykład nie zawierają podsłuchów. Tym bardziej że trafiły one do komórki, która między innymi nadaje nowe tożsamości oficerom polskiego wywiadu pracującym za granicą" – pisaliśmy.

Wcześniej aferą zakończyło się „wejście" słynnego koncernu IBM do policji oraz przebudowy rejestrów ewidencji ludności (bazy PESEL). Amerykanie bez przetargów dostali intratne kontrakty dające im dostęp do danych o milionach Polaków. Potem okazało się, że urzędnik przyznający kontrakty wziął kilka milionów złotych łapówek. W tej sprawie poza skorumpowanym urzędnikiem aresztowano i postawiono zarzuty m.in. byłym wysokim dyrektorom IBM i HP w Polsce.

Jedna z prywatnych firm wytoczyła innej amerykańskiej korporacji proces o działanie na jej szkodę m.in. poprzez wprowadzenie do oferowanego tej firmie oprogramowania kodu, który przesyłał firmowe dane do amerykańskiej spółki, działającej prawdopodobnie na zlecenie CIA. Sprawa zakończyła się ugodą.

Podane przykłady powinny skłonić polskich decydentów do refleksji: czy w wypadku najważniejszych dla państwa systemów nie powinno się stawiać na współpracę przede wszystkim z krajowymi usługodawcami, którzy podlegają pełnej kontroli polskiego prawa i służb specjalnych.

Jacek Zioło

BEZPIECZEŃSTWO INFORMATYCZNE

Najważniejsze dla zabezpieczenia fun

Polska na razie nie ma przemyślanej strategii obrony swojej cyberprzestrzeni – uważają uczestnicy **debaty DGP**

Jakie systemy informatyczne mają kluczowy wpływ na bezpieczeństwo państwa?

Piotr Niemczyk: Chodzi o systemy wymienione w ustawie o zarządzaniu kryzysowym i rozporządzeniu o ochronie infrastruktury krytycznej, które odpowiadają za działanie zaopatrzenia w energię, ciepło, wodę, gaz. Nie mniej ważne są systemy odpowiedzialne za działanie telekomunikacji, o ile warunkuje ona poprawne działanie najpierw wymienionych funkcji, a także działanie służb państwowych – wojska, policji, straży pożarnej itd. Ważne są też systemy będące podstawą funkcji sektora finansowego (np. banków).

Witold Skubina: Ważne są też te systemy, które zapewniają bezpieczeństwo obywatelom, np. teleinformatyczny i zsieciowany system ZUS, który zawiera dane np. o opłacaniu składki zdrowotnej i umożliwia korzystanie z usług publicznej służby zdrowia. Nie sposób stworzyć zamkniętego katalogu systemów o krytycznym znaczeniu dla funkcjonowania państwa, bo w tym obszarze dokonują się dynamiczne zmiany.

Michał Kamiński: Jedne systemy mają krytyczny wpływ na realizowanie relacji obywatel – państwo, a inne dla funkcjonowania samych instytucji państwa, np. łączność rządowa czy systemy do przetwarzania informacji niejawnych.

Wiesław Paluszyński: Środki komunikacji elektronicznej wyszły poza zamknięte ramy. Internet jako sposób komunikowania przekroczył założenia i plany, które towarzyszyły jego pierwszym dniom i jest dziś medium niesterowalnym, choć próby uregulowania go wciąż się pojawiają, np. grudniowe spotkanie Międzynarodowego Związku Telekomunikacyjnego (agenda ONZ) w Dubaju. W przypadku systemów informatycznych mamy do czynienia ze środowiskiem bardzo dynamicznie się zmieniającym. Warto pamiętać, że podczas wojny na Bałkanach i w Iraku celem pierwszych ataków było przerwanie przepływu informacji, ale nie przez bezpośredni atak na systemy informatyczne, lecz przez odcięcie zasilania. Z kolei przykłady blekoutów (odcięcie zasilania) w USA i Kanadzie pokazują, do czego może doprowadzić błąd ludzki i zaniechanie inwestycji w modernizację systemów infrastrukturalnych. Z drugiej strony jest to ostrzeżenie, że wkrótce blekout na dużą skalę może być wynikiem ataku na budowane obecnie inteligentne sieci energetyczne (smart grid). Atak obliczony na przerwanie odbioru energii z elektrowni atomowej może doprowadzić do katastrofy nuklearnej o skutkach trudnych do wyobrażenia. Ochrona systemów krytycznych dla państwa wymaga nie tyle ich wyspecyfikowania, ile wyspecyfikowania procedur procesów ich tworzenia i potem korzystania z nich.

Bolesław Szafrański: Żyjemy w dobie zmian tradycyjnie definiowanych pojęć. W efekcie podstawową kategorią przestało dziś być bezpieczeństwo informacji. Obecnie fundamentem bezpieczeństwa jest dostęp do systemów i dostęp do informacji. Co z tego, że pewne informacje są solidnie zabezpieczone na serwerach, skoro dostęp do tych serwerów nie jest żadną trudnością? Kto ma dostęp do serwerów, może pozbawić je sterowności i uruchomić lawinę zagrożeń.

Piotr Niemczyk: Gdy przeszło 10 lat temu pękła pierwsza bańka internetowa, Warren Buffett powiedział, że nowoczesna gospodarka to nie jest byt wyabstrahowany od pieczenia chleba, budowania domów, produkcji mebli itd. Warto trzymać się zdroworozsądkowego pojmowania bezpieczeństwa. To uchroni nas od nakręcania spirali zagrożeń, z których znaczna część będzie wirtualna, a nie realna. Należy skupić się na ochronie systemów o krytycznym znaczeniu dla państwa i oddalać pokusy uznawania, że każdy dostęp do tych systemów i potencjalne powiązanie z nimi może być źródłem niewyobrażalnej katastrofy, bo takie myślenie niczemu dobremu nie służy.

Wiesław Paluszyński: Systemy energetyczne będące wielkością zamkniętą są mniej podatne na atak z zewnątrz. Teraz budowane są inteligentne sieci. Dotychczasowy system otwiera się na wszystkich użytkowników. Oznacza to, że powstaje ryzyko ataku całego systemu energetycznego, dla którego punktem wyjścia będzie jeden inteligentny licznik.

Co jest istotne dla bezpieczeństwa obywateli, skoro wiele danych, które o nim mówią, znajduje się w systemach podlegających kontroli i ochronie państwa?

Mirosław Maj: Dla Kowalskiego krytyczne znaczenie może mieć wyciek z systemów informacji, na jaką chorobę jest Kowalski chory, ale dla bezpieczeństwa państwa ten incydent nie ma znaczenia. Jednak są też takie dane, informacje i systemy, które w przypadku przechwycenia nad nimi kontroli przez podmioty zewnętrzne, mogą spowodować w szybkim czasie paraliż państwa.

Michał Kamiński: Należy odróżnić pojęcie bezpieczeństwa państwa od bezpieczeństwa publicznego i bezpieczeństwa powszechnego. Bezpieczeństwo państwa to nie bezpieczeństwo całej populacji i każdego jej obywatela. Chodzi raczej o stan eliminacji zagrożeń dla funkcjonowania państwa i jego organów, zwłaszcza naczelnych i centralnych, i tym zajmuje się ABW.

Wiesław Paluszyński: Obecnie kluczowe znaczenie dla zabezpieczenia funkcji państwa ma wyspecyfikowanie ryzyk, przypisanie im wag, opracowanie polityki ich ograniczania i eliminowania oraz ciągłego aktualizowania tej polityki stosownie do bieżących wyzwań.

Bolesław Szafrański: W Europejskiej Agendzie Cyfrowej znajduje się sugestia, by nie wyodrębniać poszczególnych systemów i nie koncentrować się na nich, lecz tworzyć politykę bezpieczeństwa integralnego, łączącą wiele systemów współdziałających ze sobą i komplementarnych. Niemniej musi funkcjonować przypisanie danego obiektu czy procesu do strefy chronionej bądź pozostającej poza szczególną ochroną. W przeciwnym razie trudno będzie określić nawet odpowiedzialności.

Jakie systemy są istotne dla bezpieczeństwa państwa z punktu widzenia ABW?

Witold Skubina: Chodzi o systemy teleinformatyczne przetwarzające informacje niejawne.

Mirosław Maj: Jesienią br. resort cyfryzacji przekazał do konsultacji Politykę Ochrony Cyberprzestrzeni RP, która nie obejmuje systemów informacji niejawnych. Jednocześnie odwołuje się w wielu miejscach do ABW jako do podmiotu, który ma odgrywać jedną z kluczowych ról w jej realizacji.

Witold Skubina: Systemy przetwarzające informacje niejawne podlegają nadzorowi ABW na mocy ustawy. Możemy wydawać dyspozycje, jak należy je budować, zabezpieczać. W przypadku niespełnienia dyspozycji ABW system nie otrzyma wymaganej akredytacji Agencji. W przypadku Polityki Ochrony Cyberprzestrzeni RP ABW i CERT wymieniane są jako podmioty wydające zalecenia na podstawie swojej wiedzy i doświadczenia. Oznacza to, że instytucje publiczne i prywatne mogą, ale nie mają obowiązku wcielać w życie zaleceń ABW. Dlaczego? Bo chodzi o zalecenia, a nie wymagalne dyspozycje.

Mirosław Maj: Podczas ćwiczeń dotyczących ochrony infrastruktury krytycznej przed atakiem z cyberprzestrzeni – Cyber-EXE Polska 2012, we wrześniu br. doszliśmy do wniosku, że w przypadku cyberataku na system o krytycznym znaczeniu na funkcjonowanie państwa jego operator powinien mieć możliwość zgłoszenia incydentu, np. do ABW i podjęcia współpracy w celu eliminacji jego skutków. Ta współpraca nie powinna zakończyć się tylko i wyłącznie na spełnieniu obowiązku informacyjnego.

Witold Skubina: Ustawa wskazuje szefa ABW jako organ, który w przypadku wystąpienia sytuacji kryzysowej może wydawać zalecenia, ale nie polecenia czy rozkazy. Niemniej zarówno instytucje publiczne, jak i podmioty prywatne w sytuacji kryzysowej traktują te zalecenia bardzo poważnie.

Mirosław Maj: Sytuacja kryzysowa dla systemu o krytycznym znaczeniu dla państwa wymaga nie tylko miękkich zaleceń, czy rekomendacji, lecz jasnych i precyzyjnych reguł postępowania.

Witold Skubina: To jest kwestia uregulowań prawnych. Polityka Ochrony Cyberprzestrzeni RP być może nie jest dokumentem doskonałym, ale jest podstawą do dalszej pracy. Dziś poza prezydentem RP, który podjął inicjatywę nowelizacji ustawy o stanie wyjątkowym, nie znam innych aktów prawnych, które miałby wpływ na poprawę cyberbezpieczeństwa systemów o krytycznym znaczeniu dla państwa.

Wiesław Paluszyński: Jest taka regulacja prawna, o której wszyscy zapominają, choć dotyczy całej administracji publicznej. Chodzi o rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Zawiera ono cały rozdział dotyczący bezpieczeństwa teleinformatycznego. To jest jeden z lepszych aktów prawnych, który odwołuje się do nowoczesnych dobrych praktyk. Gdyby chcieć przestrzegać twardych wymogów prawnych tego rozporządzenia, a po stronie administracji publicznej nikt nic nie robi w tym kierunku, to należałoby przede wszystkim uruchomić szkolenia. Te przygotowałyby grunt pod wdrożenie postanowień rozporządzenia w życie. Skala problemu jest ogromna. Rozporządzenie obowiązuje od maja br. i jest podstawą do tego, by stworzyć w administracji publicznej podstawowy poziom zabezpieczenia systemów teleinformatycznych, kluczowych dla państwa. Przede wszystkim każdy system powinien mieć zrobioną analizę ryzyk związanych z jego obszarem funkcjonowania, a następnie trzeba je zhierarchizować i wycenić, następnie opracować procedury postępowania, system reagowania na incydenty, zasady dotyczące czynności naprawczych i raportowania oraz wskazać osoby odpowiedzialne za postępowanie zgodnie z nimi. Wtedy tak uporządkowana jednostka może odpowiadać na zalecenia wydawane przez ABW, bo nie ma układu statycznego i czekania na incydent, jak na bodziec do działania, lecz jest dynamiczny układ reagowania. Niestety instytucji publicznych, które spełniają wymagania rozporządzenia, jest bardzo mało. Spełnia je Agencja Restrukturyzacji i Modernizacji Rolnictwa. Dlaczego? Bo zgodnie z wymaganiami Unii Europejskiej wdrożenie systemu bezpieczeństwa informacji i certyfikowanie się w tym zakresie jest warunkiem korzystania z unijnych dotacji. ARiMR dzięki zabezpieczeniom może nie tylko wypłacać europejskie pieniądze, zgodnie z normami UE, ale może też szybko reagować w przypadku incydentów czy zachowań bezprawnych.

Kto jest odpowiedzialny za wdrożenie postanowień wspomnianego rozporządzenia?

Wiesław Paluszyński: Każdy kierownik jednostki administracji publicznej ma obowiązek dostosować systemy teleinformatyczne działające tam do wymagań rozporządzenia pod groźbą wyciągnięcia sankcji wynikających z niezrealizowania wymagań wynikających z obowiązujących przepisów prawnych. Gdyby nastąpiły straty z powodu niedostosowania systemów do wymagań prawa, to grozi im też odpowiedzialność karna. Dziś kierownictwo jednostek administracji publicznej nic nie robi w tym zakresie, udając, że nic nie wie o ciążącym obowiązku. Jednak jak przyjdzie co do czego, to niejeden może wylądować z zarzutami karnymi. Rozporządzenie nie narzuca sztywnych procedur, lecz określa zasady postępowania. Można budować własne systemy, pod warunkiem, że one spełnią wymagania norm opisanych w rozporządzeniu. Gdyby jednostki dostosowały swoje systemy do wymagań rozporządzenia, to wtedy łatwiej byłoby zarządzać ryzykiem lokalnie, a w konsekwencji także centralnie.

Bolesław Szafrański: Głównym skutkiem wspomnianego rozporządzenia powinno być wprowadzenie obowiązku przestrzegania zawartych tam norm zwłaszcza w przypadku tworzenia nowych systemów. Trudno te nowoczesne normy zastosować wstecz do systemów, które już działają często od wielu, wielu lat. Na to potrzebny jest czas i ogromne środki. Rozporządzenie zawiera niespodziewanie dużo bardzo cennych norm dotyczących bezpieczeństwa teleinformatycznego. Uwzględnienie wynikających z nich wymagań musi być włączone w procesy projektowania i eksploatacji systemów. Dlatego już na etapie koncepcji systemów należy brać je serio pod uwagę.

Michał Kamiński: Trzeba rozgraniczyć informacje niejawne od informacji prawnie chronionych. Do informacji niejawnych nie można zaliczyć danych osobowych i tajemnicy telekomunikacyjnej – ich ochrona jest oparta głównie na osobistej odpowiedzialności osób mających do nich dostęp z tytułu wykonywanych obowiązków. Natomiast informacje niejawne to informacje, których ujawnienie mogłoby wyrządzić szkodę państwu. W ich przypadku istnieją rozbudowane wymogi prawne odnośnie do zabezpieczenia fizycznego, w tym bezpieczeństwa teleinformatycznego – systemy teleinformatyczne, w których takie informacje są przetwarzane podlegają akredytacji przez ABW. W przypadku systemów przetwarzających dane osobowe takich wymogów nie ma, a organem odpowiedzialnym za nadzór nad prawidłowym ich przetwarzaniem jest GIODO.

Co ABW na to, że jednostki administracji publicznej nie przestrzegają wymogów omawianego rozporządzenia?

Witold Skubina: ABW nie jest policją – nie zajmuje się wszystkimi przypadkami odstępstw od wymogów obowiązującego prawa. Naszym zadaniem, zgodnie z ustawą, jest rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny. Natomiast każdy obywatel, który jest świadkiem łamania prawa i odstępstw od prawa, ma obowiązek zawiadomić o tym organa ścigania.

Witold Paluszyński: Pilnowanie, by postanowienia rozporządzenia wcielać w życie, należy do kompetencji ministra ds. cyfryzacji. Choć mamy do czynienia z rozporządzeniem Rady Ministrów, to gospodarzem tego aktu prawnego jest właśnie on. Jaka jest siła sprawcza w tym obszarze ministra ds. cyfryzacji? Brakuje nastawienia na wdrożenie postanowień rozporządzenia przez pozyskanie sojuszników w rządzie, przygotowanie programu i harmonogramu wdrażania, przeznaczenia budżetu i rozpisania odpowiedzialności. We wrześniu br. prowadziłem konferencję na temat rozporządzenia, w której udział wzięło 150 przedstawicieli administracji publicz-

Mirosław Maj:
Są takie dane, informacje i systemy, które w przypadku przechwycenia nad nimi kontroli przez podmioty zewnętrzne, mogą spowodować w szybkim czasie paraliż państwa

kcji państwa jest określenie ryzyk

„Bezpieczeństwo państwa a systemy informatyczne istotne do jego sprawnego funkcjonowania”

Wiesław Paluszyński, prezes zarządu spółki Trusted Information Consulting

Piotr Niemczyk, ekspert w sprawach służb specjalnych

dr hab. inż. Bolesław Szafrański, Wojskowa Akademia Techniczna

Witold Skubina, dyrektor departamentu bezpieczeństwa teleinformatycznego w Agencji Bezpieczeństwa Wewnętrznego

Michał Kamiński, Agencja Bezpieczeństwa Wewnętrznego

Mirosław Maj, założyciel i prezes Fundacji Bezpieczna Cyberprzestrzeń

nej z poziomów centralnego i wojewódzkiego. Z ludzi odpowiedzialnych za systemy teleinformatyczne uczestniczących w konferencji rozporządzenie znała tylko jedna osoba. Postanowienia rozporządzenia są na tyle trudne, że żadna jednostka samodzielnie nie czuje się na siłach, by się zabrać za ich wdrażanie, bez odgórnej instrukcji i koordynacji działań. W związku z tym działania pojawiają się dopiero wtedy, gdy dojdzie do incydentu i trzeba naprawić jego skutki.

Bolesław Szafrański: W każdym przypadku należy sporządzać analizy ryzyk i znaleźć środki na przeciwdziałanie przede wszystkim ryzykom największym. Bezpieczeństwo to rodzaj gry. Ryzyko zależy nie tylko od podatność systemu na zagrożenie, ale również od realności jego wystąpienia, w tym od stopnia zaangażowania i determinacji intruza. Bezpieczeństwo kosztuje. Dlatego mechanizmy i procedury ochrony muszą być adekwatne do wniosków z analizy ryzyka.

Czy systemy kluczowe dla funkcjonowania państwa są dostatecznie zabezpieczone?

Piotr Niemczyk: Trudno wyrokować, czy są zabezpieczone, czy też nie. Po pierwsze należałoby znać faktyczny stan zabezpieczeń, a po drugie analiza ryzyk, która pokazałaby, czy są chętni do zaatakowania systemów. Ogólnie nie jest dobrze, bo administracja nie jest świadoma obowiązującego prawa. Ignorancja jest tu czymś żenującym. Po drugie są agencje (ABW, CERT) będące punktem odniesienia w sprawach zabezpieczenia systemów teleinformatycznych, ale administratorzy systemów nie mają obowiązku współpracy z nimi i wdrażania ich zaleceń. Chyba wdanie się w międzynarodową awanturę mogłoby być tym kubłem zimnej wody na głowę i bodźcem do poprawienia zabezpieczeń. Pamiętajmy, że takie państwo jak Estonia, dziś stawiane za wzór pod względem zabezpieczenia systemów dla niego kluczowych, kiedyś przywiązywała jeszcze mniejszą wagę do kwestii bezpieczeństwa niż Polska. Po serii cyberataktów sytuacja uległa diametralnej zmianie.

Witold Skubina: Poziom zagrożenia systemów kluczowych dla państwa nie jest duży. Dlaczego? Bo większość tych systemów jest odizolowana od internetu, a to oznacza, że nie jest łatwym zadaniem dostanie się do nich. Atak z zewnątrz jest mniej możliwy, ale nie atak od wewnątrz. Dopóki dana organizacja nie jest wewnątrz solidnie uporządkowana, trudno mówić o bezpieczeństwie.

Michał Kamiński: W Polsce nie ma jednego organu odpowiedzialnego za bezpieczeństwo teleinformatyczne. Są jedynie odpowiedzialności wycinkowe

Mirosław Maj: Zawsze zwalczam mit odizolowanych systemów. RSA Security, znana międzynarodowa firma zaliczyła spektakularną wpadkę, która kosztowała zapewne kilkaset milionów dolarów. Włamanie do najbardziej chronionego, wewnętrznego systemu, w którym zapisano tzw. ziarna z algorytmami do tokenów tej firmy używanych na całym świecie, zostało rozpoczęte poprzez atak na jeden z biurowych desktopów, na którym otworzono odebrany e-mailem plik z arkuszem kalkulacyjnym. Lepiej jest zachować czujność i nie dać się uśpić mniemaniem (wishful thinking), że jesteśmy bezpieczni, bo systemy są odizolowane.

Bolesław Szafrański: Nie zawsze tam, gdzie rodzi się ropa, powstają technologie informatyczne, a przecież systemy jej wydobycia i przesyłania muszą być zarządzane z wykorzystaniem teleinformatyki. Wielkie i mniejsze firmy korzystają z reguły z technologii, która jest wytworzona gdzieś poza nimi, często zagranicą. Jeśli ją kupują, to zdają się z ufnością na dostawcę i zakładają, że nie sprzedaje im technologii, która oprócz spełniania umówionej funkcji wykonuje też działalność szpiegowską. Na Półwyspie Arabskim praktykuje się, że projekty realizuje nie tyle firma, która wygrała przetarg, ale kilku konkretnych jej reprezentantów. Ci przystępując do dzieła, są odizolowani od otoczenia i pracują, aż wykonają swoją pracę. Wiedza o projekcie musi, na tyle, ile to jest możliwe, pozostać u zamawiającego.

Wiesław Paluszyński: W praktyce jedna firma może zbudować system, a potem jeszcze inna utrzymywać go i nadzorować. W systemie PESEL utajony jest nie pojedynczy rekord, ale możliwość przeszukiwania tej bazy i uzyskiwania odpowiedzi przekrojowych typu: Jan Kowalski jest zamieszkały. W CEPiK niejawni są właściciele niektórych pojazdów czy uprawnienia służb w zakresie legalizacji. Ochrona tych systemów polega na uniemożliwieniu nieuprawnionym osobom dostępu do utajnionych informacji i funkcji. Trudno odpowiedzieć na pytanie czy one są bezpieczne, czy też nie. Za to bezdyskusyjna powinna być odpowiedź na pytanie: jakimi ryzykami są obarczone te systemy? Każdy system teleinformatyczny można dziś przewrócić, więc żaden nie jest bezpieczny. Za to jedne są obarczone mniejszym, a inne większym ryzykiem.

Czy zakup technologii od zagranicznych dostawców nie stwarza dodatkowego ryzyka?

Piotr Niemczyk: Na Półwyspie Arabskim nie interesują się, jak nazywa się dostawca i skąd pochodzi. Ważne jest, kto konkretnie podejmuje pracę – czy są to osoby o udokumentowanym doświadczeniu i referencjach oraz czy są one wiarygodne.

Witold Paluszyński: Znane są przypadki, w których zamawiający umawia się z dostawcą na zatrudnienie kilkudziesięciu kompetentnych ludzi do budowy systemu, a potem do jego utrzymania i rozwoju. Czas zatrudnienia jest w takich przypadkach nieokreślony, ale raczej chodzi o długie lata niż krótki okres. Polskie instytucje mają bardzo ograniczone możliwości do postępowania w ten sposób.

Bolesław Szafrański: Takie ćwiczenia jak Cyber-EXE Polska 2012 mają na celu stwierdzenie, czy systemy są i w jakim stopniu podatne na przejęcie nad nimi lub ich nad ich częściami kontroli z zewnątrz. W 1988 r. w elektrowni Turów, w wyniku awarii technicznej zniszczeniu uległ blok o mocy 200 MW i wielu urządzeń w jego otoczeniu. W tamtym przypadku przyczyną był błąd elementu automatyki. Niedawno mieliśmy do czynienia z incydentami na kolei związanymi ze skierowaniem pociągów jadących w przeciwnych kierunkach na ten sam tor. W działaniach na rzecz bezpieczeństwa chodzi o ograniczenie ryzyka wystąpienia temu podobnych incydentów przez eliminację największych ryzyk, które mogą wystąpić na skutek losowego zdarzenia, jak i w wyniku zaplanowanej akcji.

Mirosław Maj: Systemy nadzorowania i zarządzania procesami przemysłowymi, np. produkcją energii, zostały zbudowane 10–20 lat temu i rzadko kiedy się je rusza, bo jakakolwiek zmiana jest skomplikowana i może doprowadzić do wielu problemów funkcjonalnych, np. awarii zasilanie, zatrzymania ruchu pociągów czy tłoczenia gazu. Bezpieczeństwo systemu to gwarancja dostępności usługi, której jest elementem, jego poufności i integralności. Ćwiczenia Cyber–EXE Polska 2012 dowiodły, że ryzyko skutecznego na systemy przemysłowe jest jak najbardziej realne.

Witold Skubina: Dyskusja o zagrożeniach i przeciwdziałaniu im nigdy się nie kończy. Jednak rzeczywiste przeciwdziałanie zagrożeniom nieraz przekracza możliwości Agencji, jako organu, który ma prawo wydawać polecenia i zalecenia. Jesteśmy świadkami sytuacji, w której nasze zalecenia nie są przestrzegane i dalej nic nie mamy tu do zrobienia. Nie chcemy i nie możemy przeceniać naszych możliwości. Zamiast tego trzymamy się prawa.

Czy służby prowadzą nadzór nad tymi firmami polskimi i zagranicznymi, które obsługują systemy ważne dla bezpieczeństwa państwa?

Michał Kamiński: Zgodnie z ustawą zadaniem ABW jest rozpoznawanie, zapobieganie i wykrywanie przestępstw szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo i podstawy ekonomiczne państwa.

Witold Paluszyński: W tym sensie każda firma – polska i zagraniczna, jeśli podejmuje się budowy, utrzymania i rozwijania systemów o krytycznym znaczeniu dla państwa, podlega sprawdzeniu, bo musi mieć certyfikat bezpieczeństwa przemysłowego. Publicznie dostępna jest lista, na której figurują firmy sprawdzone przez służby państwa i certyfikowane. Zgodnie ze starą zasadą kryptografii zabezpieczenia są wtedy skuteczne, gdy zostaną publicznie sprawdzone. O wiele mniej skuteczne są zabezpieczenia utajnione. Kiedyś zależało mi na szybkim sprawdzeniu bezpieczeństwa schematu kryptograficznego. W Polsce musiałbym na to poświęcić ze 2 lata. Wysłałem schemat do znajomego profesora, który uczy w Chinach i ma ok. 2 tys. studentów. W ciągu 2 tygodni sprawdzili mi bezpieczeństwo algorytmu. Jeśli w wyniku testów w Chinach nie udało się złamać zabezpieczenia, to znaczy, że jest solidne.

Mirosław Maj: Systemy są na tyle bezpieczne, na ile mniejsze jest ryzyko ataku. Kraje, które swego czasu zmierzyły się za poważnymi cyberatakami, np. Estonia, Korea Płd., Iran, dziś mają modelowe zabezpieczenia. W sytuacji gdy ataku nie ma najlepszym wyznacznikiem jest posiadanie dobrej strategii ochrony. Polska na razie nie ma przemyślanej strategii obrony swojej cyberprzestrzeni i dlatego nie jest najlepiej. Proponowana przez rząd „Polityka ochrony cyberprzestrzeni RP” to niestety dokument zły i pełen błędów. Mam nadzieję, że w obecnym kształcie nie zostanie zatwierdzony, ponieważ dawałoby to złudne wrażenia, że coś już mamy. Pominięcie uwag do Polityki zgłoszonych w czasie konsultacji społecznych rodzi obawę, że nie ma woli poprawiania tego dokumentu.

Witold Paluszyński: Państwo jest bezpieczne, gdy jego systemy są solidnie przeanalizowane pod kątem ryzyk, poddane rygorowi procedur bezpieczeństwa. Potrzebna jest wspomniana strategia, którą będzie można zweryfikować i poprawiać we współpracy z przedsiębiorcami i naukowcami.

Bolesław Szafrański: W Polsce dopiero rodzi się kultura prywatności – łatwo dzielimy się informacjami o sobie. Każda próba wprowadzenia ograniczeń ze względów bezpieczeństwa budzi sprzeciw jako naruszająca wolność. Potrzebna jest umiejętność dowiedzenia, że bez przyjęcia pewnych ograniczeń możemy popaść w dużo większe ograniczenie wolności.

Michał Kamiński: W Polsce nie ma jednego organu odpowiedzialnego za bezpieczeństwo teleinformatyczne. Są jedynie odpowiedzialności wycinkowe. Brakuje natomiast centrum koordynującego zabezpieczenie polskiej cyberprzestrzeni.

Witold Skubina: W Polityce Ochrony Cyberprzestrzeni RP zawarta jest propozycja powołania zespołu koordynującego działania na poziomie centralnym, regionalnym i lokalnym.

Debatę prowadził Marcin Piasecki, wydawca DGP. Relację przygotował Krzysztof Polak

Cyberwojna cofnęłaby nas do etapu konnych zaprzęgów

Jewgienij Kasperski: Światowe mocarstwa liczą się z realnym zagrożeniem i rozwijają własne arsenały cyberbroni

Dostęp do internetu jest coraz szerszy, korzystanie z niego coraz powszechniejsze. Jak to zmienia podejście państw i użytkowników?

Wkroczyliśmy w trzeci etap ewolucji internetu – etap regulacji. Na pierwszym etapie innowacji globalna sieć stawała się coraz bardziej dostępna, na drugim –incydentów – użytkownicy zdali sobie sprawę i doświadczali, że korzystanie z internetu wiąże się niebezpieczeństwem. W dużej mierze nadal znajdujemy się na etapie incydentów. Jednak etap regulacji już następuje, mimo że jest to dopiero początek. Wiele państw posiada już zespoły CERT (Computer Emergency Response Team) i ustawy o cyberprzestępczości. Jednak na drodze do egzekwowania prawa stoi często brak wystarczających środków oraz zasobów, co utrudnia walkę z cyfrowymi zagrożeniami.

Jak przeciwdziałać cyberszpiegostwu i cyberagresji?

Z roku na rok jest coraz bardziej jasne, że zwalczanie cyberprzestępczości to nie jest zadanie, któremu może sprostać samodzielnie jakakolwiek organizacja. Wynika to stąd, że cyberprzestępczość przekracza granice geopolityczne – przecież cyberagresorzy mogą sobie obrać za cel użytkowników znajdujących się na drugim

Jewgienij Kasperski, założyciel i dyrektor generalny Kaspersky Lab

końcu świata. W przeciwieństwie do nich organy ścigania podlegają ograniczeniom jurysdykcyjnym i nie mogą samodzielnie przeprowadzać dochodzeń poza granicami swego państwa. Logiczne jest zatem pójście w kierunku współpracy między krajami na obszarze wspólnego przeciwdziałania cyberprzestępczości.

Od kilku lat cybernetyczne działania wojenne są kwestią wzbudzającą największe zaniepokojenie wśród ekspertów z dziedziny bezpieczeństwa IT, szczególnie od czasu wykrycia Stuxneta w 2010 roku i Duqu w 2011 roku. Odkrycie Flame w 2012 roku jeszcze bardziej zwiększyło te obawy – dowiodło, że broń cybernetyczna może zostać użyta przeciwko każdemu państwu. Flame to wysoce zaawansowany zestaw narzędzi do przeprowadzania ataków o sile rażenia dwudziestokrotnie większej niż Stuxnet. W tym kontekście pogłębianie globalnej współpracy można uznać za jedno z głównych wyzwań obecnych czasów.

Jak działają takie cyberbomby?

Stuxnet i Duqu stanowią próbkę technicznego zaawansowania złośliwego oprogramowania mającego potencjał cybermilitarny. Takie programy potrafią uszkodzić duże instalacje przemysłowe i nie tylko. Szkodniki te burzą spokój i pewność co do bezpieczeństwa internetowego – zarówno Stuxnet, jak i Duqu zostały wykryte przez przypadek po pewnym czasie od ich stworzenia. Wykrycie robaka Stuxnet wywołało panikę na świecie. Kilka państw przyrównało skutki użycia tej cyberbroni do wyników zastosowania konwencjonalnych działań wojennych obejmujących bombardowania pociskami wystrzeliwanymi z lądu i bombami zrzucanymi z powietrza. Nic dziwnego, że w 2011 roku prawie wszystkie duże państwa na świecie dały do zrozumienia, że liczą się z cyberatakami i w związku z tym nastawiają się na rozwój oraz stosowanie własnych arsenałów cybernetycznych.

Czym jest cyberwojna?

W szerszej perspektywie cyberwojna jest grą, w której wszystkie strony przegrywają: napastnicy, ofiary, a nawet niezaangażowani obserwatorzy. W odróżnieniu od tradycyjnej broni narzędzia użyte w ramach cyberwojny mogą zostać w łatwy sposób sklonowane i przeprogramowane przez wrogie siły. Ich użycie zagraża działaniu cybernetycznych infrastruktur sieciowych w sektorze energetycznym, finansowym, telekomunikacyjnym oraz rządowym na całym świece. Najważniejszym zadaniem, od którego realizacji zależy przetrwanie cyberwojny, jest opracowanie i wdrożenie nowego, zaawansowanego modelu bezpieczeństwa dla najbardziej krytycznych infrastruktur. Nie możemy pozwolić, aby działania cyberwojenne wstrzymywały rozwój ludzkości.

30 lat temu obawiano się konfliktu nuklearnego, który mógł zniszczyć naszą planetę. Ale wojna w cyberprzestrzeni to inny rodzaj zagrożenia.

Dla mnie to przerażająca, apokaliptyczna wizja! Gdyby spełnił się jeden z najgorszych scenariuszy cyberwojny, moglibyśmy cofnąć się o setki lat – transport konny, czytanie papierowych książek, tradycyjna poczta czy oświetlenie przy pomocy świec. Najgorsze jest to, że obecnie jesteśmy dość bezsilni wobec tego rodzaju ataków. Konieczne jest przeprojektowanie całego oprogramowania dla systemów przemysłowych, ale to może zająć 10–20 lat i stanowić swego rodzaju „mission impossible".

W tym roku Komisja Europejska zaproponowała stworzenie europejskiego centrum ds. cyberprzestępczości. To pomoże?

Propozycja Komisji Europejskiej to wspaniała inicjatywa, którą przyjmuję z entuzjazmem. Brak tego rodzaju międzynarodowej współpracy odczuwamy od kilku lat, w miarę jak nasze życie cechuje coraz większa mobilność i cyfrowość. Nie jest to pierwsza inicjatywa tego typu – istnieją już dwie duże organizacje, które pretendują do objęcia dowodzenia w walce z cyberprzestępczością na poziomie międzynarodowym: Action Against Terrorism Unit w ramach Organizacji Narodów Zjednoczonych oraz Interpol, który planuje otworzyć oddział Cyber Interpol w Singapurze w 2014 roku. Jednak im więcej organizacji w tym obszarze, tym lepiej. Cyberzagrożenia dotyczą nie tylko rządów państw i potężnych firm, ale także każdego z nas. Priorytetem jest eliminacja zagrożenia cybernetycznego, by nie wpływało na działanie krytycznej infrastruktury. Cel ten musi zostać zrozumiany i przyjęty przez wszystkie zainteresowane strony na poziomie międzynarodowym.

Rozmawiał Krzysztof Polak

Chińskie koncerny mogą być wykluczone z przetargów publicznych w Stanach Zjednoczonych

Kongres USA wskazuje na możliwość **zagrożenia bezpieczeństwa** Stanów Zjednoczonych

Komisja ds. wywiadu (House Intelligence Committee of US) po roku pracy, m.in. przesłuchań przedstawicieli największych chińskich producentów sprzętu telekomunikacyjnego – ZTE Corp i Huawei Technologies opublikowała raport. Ma on charakter wstępny, ale zawiera niezwykle poważne ostrzeżenia i zalecenia. Komisja uważa, że Huawei i ZTE powinny otrzymać zakaz stawania do przetargów publicznych na rynku amerykańskim, zwłaszcza w projektach, w których zakłada się przetwarzanie danych wrażliwych. Wnioskuje też, by amerykańska administracja blokowała wszelkie przejęcia czy fuzje planowane przez obie firmy. Dlaczego? Ze względu na możliwość szpiegostwa przemysłowego i wojskowego. Komisja amerykańskiego kongresu wnioskuje też o rozpoczęcie osobnego śledztwa w tej sprawie.

Oba chińskie koncerny stanowczo zaprzeczają podejrzeniom kongresmenów. Bill Plummer, rzecznik prasowy Huawei, podkreśla, że firma nie stosuje żadnej formy szpiegostwa.

Mur podejrzeń

Około 4 proc. swoich ubiegłorocznych przychodów Huawei wypracował w USA. W przypadku ZTE ten odsetek przychodów wyniósł 2,5 proc. Obie firmy współpracują na amerykańskim rynku z największymi tamtejszymi operatorami telekomunikacyjnymi: Verizon, Sprint i T–Mobile USA. W ciągu minionego dziesięciolecia obaj chińscy dostawcy urządzeń telekomunikacyjnych i telefonów komórkowych weszli do pierwszej dziesiątki globalnych potentatów w tych branżach. Biorąc pod uwagę wartość przychodów za pierwsze półrocze 2012 r., Huawei zdobyło pierwsze miejsce w rankingu największych dostawców sprzętu telekomunikacyjnego, dystansując szwedzkiego Ericssona. ZTE uplasowało się w tym zestawieniu na piątym miejscu. Z kolei na rynku producentów telefonów komórkowych ZTE zdobyło czwartą pozycję, a Huawei szóstą – wynika z danych firmy analitycznej Gartner.

Jednocześnie rok 2012 był dla obu firm pierwszym, w którym musiały stawić czoła podejrzeniom o szpiegostwo i zagrożenie bezpieczeństwa teleinformatycznego w USA, Australii i Wielkiej Brytanii.

Również Komisja Europejska rozważa możliwość wszczęcia oficjalnego postępowania w sprawie legalności rynkowych praktyk obu koncernów. Powodem są podejrzenia o przyjmowanie przez firmy subwencji od chińskiego rządu, dzięki którym łatwiej wygrywają z europejskimi dostawcami sprzętu telekomunikacyjnego. Komisja chce wziąć pod uwagę skargi czołowych graczy na tym rynku. Ci już od dawna narzekają, że za sprawą polityki handlowej stosowanej przez ZTE i Huawei ceny profesjonalnych urządzeń telekomunikacyjnych zbyt szybko spadają. Ich zdaniem obniżki są szybsze, niż wynikałoby to z rozwoju rynku. Łączny udział dwóch firm z Chin w rynku europejskim wynosi obecnie około 25 proc (w 2006 r. było to 2,5 proc.). Wzmacnianie pozycji chińskich dostawców sprawi, że ich europejscy konkurenci zostaną zmuszeni do zamknięcia swoich linii produkcyjnych, co zwiększy stopień zależności UE od sprzętu produkowanego w Chinach.

Wzmacnianie pozycji chińskich dostawców sprawi, że ich europejscy konkurenci zostaną zmuszeni do zamknięcia swoich linii produkcyjnych, co zwiększy stopień zależności UE od sprzętu produkowanego w Chinach

Groźne luki

We wrześniu rząd Australii wykluczył Huawei z udziału w licytowaniu umów na rozbudowę sieci szerokopasmowego internetu. W uzasadnieniu wskazał, że ma „obowiązek zrobić wszystko, aby chronić integralność tej sieci". Komentatorzy uważają, że jest to konsekwencja podejrzeń, jakie amerykańscy kongresmeni wysunęli wobec Huawei i ZTE oraz wskazania ich jako firm, z którymi Amerykanie nie powinni robić interesów. Nie bez znaczenia jest też fakt, że latem 2012 r. niemieccy eksperci z firmy Recurity Labs przeprowadzili druzgocącą krytykę zabezpieczeń routerów Huawei. Felix Lindner i Gregor Kopf ostro skrytykowali też jakość zainstalowanego na tych urządzeniach oprogramowania. Odkryte luki w zabezpieczeniach mogą być wykorzystane do przeprowadzenia zdalnego ataku. Specjaliści podkreślali, że te błędy są „najgorszymi, jakie widzieli od dawna".

Z kolei pracujący m.in. dla Pentagonu analityk F. Michael Maloof twierdzi, że Chińczycy mogą szpiegować nawet 80 proc. światowej komunikacji. Jego zdaniem Huawei i ZTE utworzyły w swoim sprzęcie furtkę, przez którą chińska armia zdobywa dane. Maloof twierdzi, że do telekomunikacyjnego monitoringu dochodzi w 140 krajach świata, bo z urządzeń Huawei i ZTE korzysta 45 z 50 największych światowych telekomów.

Przedstawiciele Huawei obruszają się, że w USA mają do czynienia z niepopartymi dowodami spekulacjami. John Lord, prezes australijskiego oddziału Huawei, obiecał, że Huawei da australijskim władzom pełny i nieograniczony dostęp do swojego sprzętu i kodu źródłowego oprogramowania. Zaproponował też, by Australia stworzyła centrum ewaluacji cyberbezpieczeństwa.

Pytania o bezpieczeństwo

W Wielkiej Brytanii Huawei testuje sprzęt i oprogramowanie. Prace te prowadzi w laboratorium podległym brytyjskiemu rządowi. Jednak po wydarzeniach mijającego roku brytyjscy politycy zapowiadają, że bacznie się przyjrzą działalności chińskiego koncernu na lokalnym rynku.

W Nowej Zelandii opozycja wprost wezwała do odsunięcia Huawei od budowy sieci ogólnokrajowego szerokopasmowego internetu, wskazując, że decyzja władz w Australii powinna być brana za wzór. Podobne głosy pojawiły się w Kanadzie.

Przedstawiciele Huawei i ZTE konsekwentnie zaprzeczają, że rząd Chin ma jakikolwiek wpływ na to, co dzieje się w tych przedsiębiorstwach.

Krzysztof Polak