Nr 1 - Czerwiec 2012

CIP focus

RCB
Rządowe Centrum Bezpieczeństwa

informator o ochronie teleinformatycznej

STUXNET

studium przypadku

W lipcu 2010 roku świat internetowy obiegła informacja o wykryciu nowego, groźnego wirusa komputerowego. Nadano mu nazwę Stuxnet. Jak jest zbudowany, jak działa, kto jest jego twórcą, kogo miał zaatakować i dlaczego w annałach historii złośliwego oprogramowania zapisał się jako jeden z najbardziej niebezpiecznych wirusów działających w systemach sterujących instalacjami przemysłowymi?

Analiza na str. 3

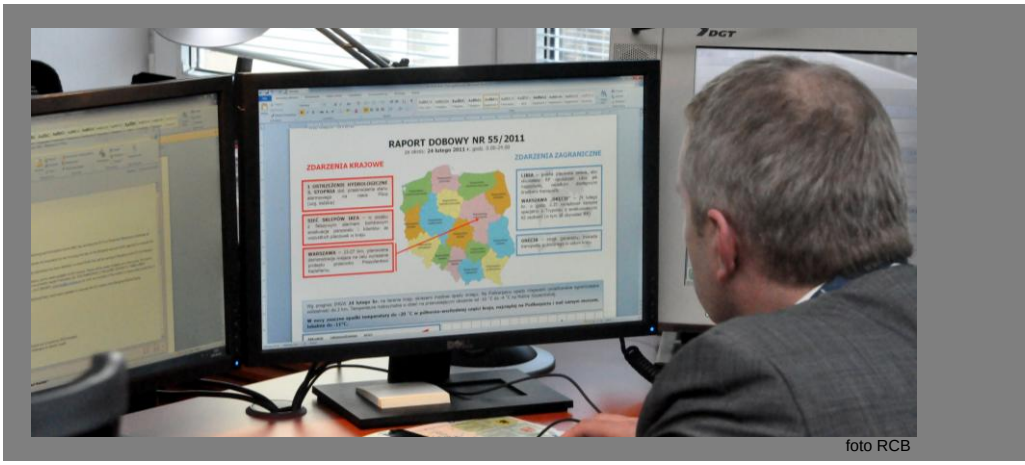


foto RCB

foto RCB

Infrastruktura krytyczna to termin nadużywany

Dyrektor Rządowego Centrum Bezpieczeństwa Marek Komorowski o cyberprzestrzeni, infrastrukturze krytycznej, sposobach i programach jej ochrony, a także o istocie współpracy i wzajemnym zaufaniu.

Wywiad str. 8

CERT Center

CERTy idea i historia

CERT - Zespół Reagownia na Przypadki Naruszenia Bezpieczeństwa Teleinformatycznego. Czy taka forma zarządzania incydentem w cyberprzestrzeni sprawdza się oraz czy warto stworzyć we własnej firmie lub instytucji swój CERT? Rozpoczynamy serię artykułów w dziale CERT Center.

Czytaj str. 6

Ochrona Teleinformatyczna Infrastruktury Krytycznej

26 kwietnia, na konferencji poświęconej ochronie systemów komputerowych spotkali się operatorzy kluczowej dla funkcjonowania państwa infrastruktury oraz reprezentanci administracji publicznej.

Sprawozdanie str. 11

Drodzy Czytelnicy,

Oddajemy w Wasze ręce pierwszy numer informatora poświęconego teleinformatycznej ochronie infrastruktury krytycznej. Informator zatytułowaliśmy „CIIP focus". CIIP to powszechnie używany akronim od Critical Information Infrastructure Protection, czyli terminu używanego dla szeroko rozumianej tematyki teleinformatycznej ochrony infrastruktury krytycznej, ale również używanego do określenia infrastruktury krytycznej w sektorze technologii informacyjno-komunikacyjnych. My będziemy się koncentrować na pierwszym znaczeniu.

Jesteśmy przekonani co do tego, że nadszedł czas na systematyczne zajmowanie się tym tematem, a zawarte w niniejszym Informatorze publikacje będą pomocne w jego bliższym poznawaniu, uświadamianiu ważnych kwestii, jak również stanowić będą praktyczny przewodnik we wprowadzaniu i poprawianiu rozwiązań z zakresu bezpieczeństwa IT w Państwa organizacjach.

Pierwszy numer jest wyznacznikiem tego jak na dzień dzisiejszy wyobrażamy sobie Informator. Z pewnością jego kształt będzie ewaluował. Będziemy dynamicznie odpowiadać na to co w temacie CIIP jest najważniejsze, jakie pojawiają się potrzeby związane z rozwijaniem skutecznej współpracy pomiędzy sektorem prywatnym i sektorem administracji państwowej i wreszcie, co właściwie jest dla nas najważniejsze, jakie będą Państwa oczekiwania wobec zawartych w Informatorze publikacji.

Jeśli ktoś chciałby bliżej zapoznać się z misją naszego działania, to chyba najlepiej ujmuje ją wywiad z Dyrektorem RCB - Markiem Komorowskim, w którym wyjaśnia on szczegółowo rolę RCB w ochronie teleinformatycznej infrastruktury krytycznej oraz założenia Narodowego Programu Ochrony Infrastruktury Krytycznej. Oprócz wywiadu zachęcamy do zapoznania się z historią, miejscami tajemniczą, najsłynniejszego robaka atakującego systemy SCADA, czyli Stuxneta oraz pierwszym odcinkiem cyklu o CERT-ach (Computer Emergency Response Team). Być może niektórzy z Czytelników znajdą siebie na zdjęciach i w relacji z ciekawej konferencji jaka odbyła się pod koniec kwietnia w siedzibie PSE Operator SA, a którą współorganizowało RCB. Do całości dodajemy krótkie informacje z odsyłaczami do szerszej lektury. Tam też można znaleźć wiele pożytecznych wskazówek i najświeższych tematów, jak chociażby informacje o słynnym w ostatnich tygodniach wirusie Flame.

Zachęcamy do lektury i do wyrażenia opinii o Informatorze oraz nadsyłania własnych propozycji tematów, które widzieliby Państwo na łamach naszego periodyku. Te sugestie i opinie będą dla nas bardzo ważne w ustalaniu zawartości następnych numerów „CIIP focus". Nic zresztą nie stoi na przeszkodzie, aby w przyszłości powstał dział „Listy od Czytelników".

Tymczasem uruchomiliśmy adres mailowy ciip-focus@rcb.gov.pl. Mogą Państwo kierować na niego swoje uwagi, a także propozycje dotyczące zawartości naszego Informatora. Mile będziemy widzieć również artykuły lub inne publikacje.

Redakcja

Jeśli nie zaznaczono inaczej, fotografie pochodzą z serwisu: http://www.publicdomainpictures.net

NEWS

Indie inwestują w ochronę infrastruktury krytycznej

Rząd Indii zdecydował się na inwestycję w ochronę teleinformatyczną. Wprowadził również autoryzację dla dwóch agencji rządowych do przeprowadzania ataków sieciowych w przypadku zajścia takiej konieczności. Te strategiczne zmiany są między innymi wynikiem stosunkowo wielu infekcji w Indiach groźnym Stuxnetem. Mimo, że jak wiadomo sam wirus był nastawiony na ataki tylko na instalacje irańskie (piszemy o tym dokładnie w artykule o wirusie Stuxnet).

http://bit.ly/LKpzyn

Bezpieczeństwo teleinformatyczne w czasie olimpiady w Londynie

W trakcie olimpiady w Pekinie organizatorzy doświadczali milionów ataków informatycznych dziennie. Zaraz po jej zakończeniu komputerowi przestępcy przystąpili do operacji „Londyn 2012". O tym jakiego typu są to ataki i jak jest zorganizowana ochrona przed nimi można przeczytać w serwisie Infosec Island oraz w biuletynie amerykańskiego Departamentu Bezpieczeństwa Wewnętrznego (Department of Homeland Security).

http://bit.ly/KqTVbg
http://bit.ly/KE3xuR

Ochrona krytycznych zasobów na przykładzie placówek medycznych

W magazynie „Hospital Review" pojawiła się publikacja na temat 9 podstawowych zasad dotyczących bezpieczeństwa w placówkach medycznych. Autorzy w szczególny sposób uwzględniają fakt, że żyjemy w środowisku, w którym powszechny jest praktyka BYOD (Bring Your Own Device) i BYOC (Bring Your Own Cloud). Implikuje to wiele problemów, którym trzeba zaradzić. Propozycja radzenia sobie z nimi zawiera głównie rozwiązania organizacyjne. Co prawda są one zwrócone do sektora medycznego, niemniej jednak są na tyle uniwersalne, że inni użytkownicy, również operatorzy teleinformatycznej infrastruktury krytycznej, mogą z powodzeniem je wykorzystać.

http://bit.ly/LmzoBl

STUXNET TRAFIA NA LISTĘ NAJGROŹNIEJSZYCH WIRUSÓW

STUXNET

studium przypadku

W lipcu 2010 roku świat internetowy obiegła informacja o wykryciu nowego, groźnego wirusa komputerowego. Nadano mu nazwę Stuxnet.

Odkrycia dokonała białoruska firma zajmująca się bezpieczeństwem teleinformatycznym – VirusBlokAda. Stało się to w trakcie analizy komputerów jednego z klientów tej firmy, który pochodził z Iranu. Badając komputer, specjaliści z VirusBlokAda natrafili na coś zupełnie nowego. To, co czyniło Stuxneta innym od wielu jego poprzedników był fakt, że miał on za cel atak na systemy przemysłowe, powszechnie nazywane systemami SCADA (Supervisory Control And Data Aquisition), które odpowiedzialne są za nadzorowanie przebiegu procesów technologicznych w przedsiębiorstwach. Jak się później okazało, szczególnym celem działania wirusa było naruszenie procesu technologicznego, związanego ze sterowaniem pracy wirówki odpowiedzialnej za wzbogacanie uranu, co w skrajnym przypadku może doprowadzić nawet do jej wybuchu. Już chociażby z tego względu wirus trafił na listę najbardziej niebezpiecznych i znanych wirusów w historii. Szczegółowa analiza działania wirusa oraz inne okoliczności, związane chociażby z historią jego powstania, tylko i wyłącznie ugruntowały pozycję Stuxneta na takiej liście. Wiele pytań, na które do dziś nie ma odpowiedzi, budują wokół Stuxneta dodatkową aurę tajemniczości.

KOGO MIAŁ ZAATAKOWAĆ STUXNET?

Jeśli spojrzeć na mapę lub listę państw, w których wykryto najwięcej infekcji Stuxnetem, to zdecydowanie na pierwsze miejsce wybija się Iran. W kilku innych państwach również wykryto znaczące ilości infekcji, np.: w Indonezji około 20%, ale to właśnie w Iranie było ich najwięcej. Różne szacunki pokazują, że było to około 60% wszystkich infekcji. Na liście są również inne państwa – Indie, Azerbejdżan, Chiny, Stany Zjednoczone, Korea, Wielka Brytania. W ciągu kilku pierwszych tygodni działania wirusa, specjaliści firmy Symantec wykryli około 14 000 połączeń do serwera kontrolującego działanie wirusa, co odpowiada liczbie infekcji w tym okresie. Na koniec września 2010 roku, kiedy to doszło już do większości infekcji, wyliczono je na około 100 000. Rozkład geograficzny ataków nie był przypadkowy, gdyż głównym celem ataku były systemy przemysłowe w Iranie, a tak naprawdę – jak wykazała to późniejsza szczegółowa analiza kodu – systemy zlokalizowane w irańskim zakładzie wzbogacania uranu w Natanz, który pełni kluczową rolę w całym irańskim programie nuklearnym. Zresztą zdaniem wielu specjalistów to właśnie cały program miał być celem ataku. Korzystając ze złośliwego oprogramowania atakującego system Windows, poprzez kontrolery przemysłowe PLC (ang. Programmable Logic Controller), atak skierowany był na cały zakład wzbogacania uranu, a w konsekwencji na cały irański program nuklearny.

JAK ZBUDOWANY JEST I JAK DZIAŁA STUXNET?

Kod Stuxneta to zdaniem specjalistów prawdziwy programistyczny majstersztyk. 15 000 linii kodu zawiera wyrafinowane funkcje i jest dowodem nie tylko na najwyższą klasę specjalistów biorących udział w jego przygotowaniu, ale również na ich dostęp do poufnych informacji, które zostały wykorzystane przy pisaniu kodu wirusa.

Co tak naprawdę robił Stuxnet? Analizy dokonało wielu specjalistów. Chyba najbardziej znane są te, przygotowane przez firmy Symantec i Langner Communications. Symantec opublikował szczegółowy, kilkudziesięciostronicowy raport z analizy, zaś Ralph Langner zasłynął swoją kilkuminutową prezentacją w czasie cyklu popularnych konferencji TED, w trakcie której wskazuje na Izrael i Stany Zjednoczone, jako tych którzy są odpowiedzialni za przygotowanie Stuxneta. Obydwie analizy potwierdzają, że Stuxnet nie jest przypadkowym wirusem, który miał infekować przypadkowe komputery. Jest to bardzo skomplikowany kod, który zawierał cztery tzw. 0-days[1]. Jego podstawowy algorytm

działania jest następujący: po instalacji wirusa, która dochodzi zazwyczaj przez przeniesienie go do systemu z pamięci USB, wirus rozprzestrzenia się w sieci LAN samodzielnie poprzez wykorzystanie różnych słabości systemowych, np.: w usłudze drukowania w sieci lokalnej (Windows Print Spooler). Następnie wirus rozpoczyna poszukiwanie sterownika PLC. Sterownik nie jest przypadkowy, ponieważ chodzi o sterownik firmy Siemens SIMATIC WINN/STEP 7. Próba przejęcia kontroli nad nim następuje poprzez wykorzystanie domyślnego hasła producenta. Jak wiadomo stosowanie domyślnych haseł do urządzeń jest powszechnym i bardzo niebezpiecznym zjawiskiem. Kiedy próba jest udana następuje kluczowa i najbardziej niebezpieczna operacja. Wirus przejmuje prawdziwe dane dostarczane z mierników urządzeń przemysłowych i podmienia je wysyłając dane sfałszowane. Z punktu widzenia zagrożeń generycznych jest to klasyczny spoofing. Ten spoofing prowadzi do manipulacji działania wirówek i zaworów. Całość ataku jest koordynowana poprzez łączność z serwerem nadzorującym. Właśnie łączność z serwerem nadzorującym pozwoliła na identyfikację zainfekowanych komputerów, a przede wszystkim przejęcie kontroli nad serwerem, tak aby dalsze złośliwe działanie nie było możliwe. Swoją drogą jeśli już gdzieś szukać błędów w przygotowaniu wirusa, to chyba właśnie najbardziej dotyczyły one modelu zarządzania sieciowego i zdalnego. Po wytypowaniu zainfekowanych komputerów, co można dokonać na podstawie analizy ruchu sieciowego, można wirusa usunąć z systemu. Nie oznacza to jednak, że staje się on nieszkodliwy. Specjaliści z Symanteca ostrzegają, że nawet po jego usunięciu może się okazać, że zostawił on w komputerze niebezpieczne polecenia, które w pewnym momencie mogą zostać wykonane. Dlatego jedynym słusznym działaniem jest albo reinstalacja systemu, albo przywrócenie bezpiecznej kopii zapasowej z okresu przed infekcją.

Skąd jednak wiadomo, że wirus był nastawiony na zaatakowanie systemów w Iranie? Dość obrazowo sprawę przedstawił Ralph Lengner, który powiedział następujące zdanie: „Kiedy wypuściliśmy Stuxneta w naszym laboratorium, to zachowywał się jak mysz laboratoryjna, która nie lubi naszego sera". Chodziło o to, że kod Stuxneta był tak precyzyjnie napisany, że interesował go atak tylko na szczególne instalacje przemysłowe o bardzo precyzyjnie zdefiniowanej strukturze. W kodzie powtarzała się tajemnicza liczba 164, która okazała się programistycznym odwołaniem do liczby wirówek w jednej z 6 kaskad, z których zbudowane są zakłady wzbogacania uranu w Natanz. Krótko mówiąc Stuxnet może i był zainstalowany na wielu komputerach na całym świecie, ale uaktywniał się tylko tam gdzie wykrywał specyficzną, interesującą go, konfigurację.

[1] rodzaj zagrożenia, który nie jest jeszcze znany producentowi oprogramowania i na który nie wyprodukowano jeszcze zabezpieczenia.

NEWS

Flame – nowy bardzo groźny wirus

Niespełna dwa lata po wykryciu wirusa Stuxnet wykryto wirus Flame, który jest niezwykle zaawansowanym narzędziem do kradzieży danych z zainfekowanych komputerów. W momencie jego działania żaden z 43 czołowych programów antywirusowych nie był w stanie wykryć wirusa Flame. Dość szczegółową analizę wirusa przeprowadził CERT irański. Irańczycy twierdzą, że to kolejny po Stuxnecie cybernetyczny atak skierowany przeciwko nim.

http://bit.ly/LL9NTu
http://bbc.in/Kzx1uZ

Pierwsze polskie ćwiczenia z ochrony w cyberprzestrzeni

W Polsce przygotowywane są pierwsze ćwiczenia z ochrony infrastruktury krytycznej przed zagrożeniami z cyberprzestrzeni. 19 września we Wrocławiu kilkunastu reprezentantów sektora administracji państwowej i sektora właścicieli infrastruktury przećwiczy swoje procedury reagowania na przypadku ataku na IK. Ćwiczenia przygotowywane są przez kilka miesięcy przez specjalny zespół, a organizatorzy dostali wsparcie Europejskiej Agencji Bezpieczeństwa Sieci i Informacji – ENISA.

http://bit.ly/Kw0z0eI

Jak reagować na najpoważniejsze ataki z sieci

Z raportu McAfee dotyczącego ochrony infrastruktury krytycznej wynika, że 80% doświadczyło ataków typu DDoS, a 85% ataków związanych z penetracją sieci wewnętrznych. Jak reagować na takie ataki. Czy kontratak sieciowy jest dobrym i skutecznym pomysłem? Jak administracja państwowa powinna zadbać o odpowiedni poziom ochrony teleinformatycznej infrastruktury krytycznej? Rozważania na ten temat prowadzi specjalista z dziedziny ochrony TIK - William McBorrough.

http://bit.ly/M70AmW

Stuxnet został wykryty w lipcu 2010 roku. Jednak dzisiaj już wiemy, że praca nad nim trwała znacznie wcześniej, a pierwsze ślady pochodzą już z czerwca 2009 roku. Natomiast pierwsze ataki i infekcje nastąpiły na początku 2010 roku. Zresztą śledzenie rozwoju Stuxneta to bardzo ciekawe zajęcie. Kolejne jego wersje wskazują na intensywne prace i coraz bardziej zaawansowany kod. Szczególnie ciekawe są moduły służące do utrudniania wykrywania Stuxneta, które zostały dodane na początku 2010 roku. Zawierają one podpisy cyfrowe złośliwego oprogramowania, które zostały wykonane skradzionymi certyfikatami dwóch tajwańskich firm - Realtek i JMicron. Podpisy oprogramowania uwiarygodniały złośliwe oprogramowanie, co w rezultacie prowadziło do utrudnienia jego wykrycia. Długo można by jeszcze pisać o zaawansowaniu i zawiłości kodu Stuxneta. Dobrym podsumowaniem tych informacji niech będzie zdanie wypowiedziane przez Roela Schouwenberga z zespołu badawczego Kaspersky Lab: „Bez żadnej wątpliwości to jest z pewnością najbardziej zaawansowany atak dedykowany jaki do tej pory widzieliśmy".

KTO JEST TWÓRCĄ STUXNETA?

Kto więc jest twórcą tego spektakularnego i tak niebezpiecznego oprogramowania? To z pewnością najbardziej tajemnicza części dossier Stuxneta, choć większość specjalistów ma swoich mocnych „podejrzanych". Zacznijmy od tego, że stworzenie Stuxneta wiązać się musiało z niemałą inwestycją. Nie wszystkich jest na to stać. A już z pewnością nie każdy ma dostęp do poufnych informacji, które zostały wykorzystane przy pisaniu kodu. Generalnie rzecz biorąc trzeba się zgodzić ze wspomnianym już Roelem Schouwenbergiem, że Stuxneta musiało przygotować jakieś państwo. Bardziej precyzyjni są inni badacze Stuxneta. Badający szczegółowo kod Stuxneta – Ralph Lengener, twierdzi że w przygotowaniu Stuxneta wziął udział izraelski Mossad i Amerykanie. Co prawda nie wyjaśnia on szczegółowo swoich przypuszczeń, ale trudno się nie zgodzić z tym, że motyw w tym wypadku jak najbardziej istnieje – obydwa państwa są żywo zainteresowane w powstrzymaniu irańskiego programu atomowego.

Na początku czerwca 2012 roku amerykański The New York Times opublikował artykuł Davida Sangera, w którym autor twierdzi, że Stuxnet to wynik amerykańskiego tajnego programu nazwanego „Olympic Games". Rozpoczęła go jeszcze administracja prezydenta Georga Busha, a kontynuuje administracja obecnego prezydenta – Baracka Obamy. Program ten ma polegać na zaawansowanych atakach komputerowych na irańskie instalacje atomowe. Opowieść o tym jak do tego doszło to fragment książki Sangera – „Confront and Conceal", opisującej kulisy całej historii. Historia politycznych powiązań ze Stuxnetem posiada jeszcze więcej niewyjaśnionych historii, jak chociażby śmierć irańskiego eksperta, który przewodniczył badaniom nad Stuxnetem – profesora Majida Shahriariego.

Niewątpliwie, niezależnie od tego co naprawdę wiemy i co potrafimy udowodnić w sprawie twórców Stuxneta – jest to przykład cyber-broni, która co raz częściej pojawia się w arsenale światowych mocarstw. Atak Stuxnetem na tak istotne instalacje przemysłowe pokazał, że w cyberprzestrzeni odbywa się prawdziwy konflikt z wykorzystaniem bardzo groźnych narzędzi. Konsekwencje ataku na system SCADA mogą być nie tylko elementem wyrafinowanej, skrytej gry pomiędzy największymi tego świata, ale mogą one spowodować całkiem realne i dotkliwe zagrożenia dla zwykłych obywateli. Systemy SCADA kontrolują coraz więcej systemów odpowiedzialnych za codzienne funkcjonowanie infrastruktury. Za dostawę prądu czy gazu lub kontrolę ruchu kolejowego. Atak Stuxnetem to swego rodzaju atak generyczny. Przykład czegoś co wcześniej nie występowało, a co niestety może się zdarzać coraz częściej. Dlatego zabezpieczenie systemów nadzorujących działanie infrastruktury krytycznej staje się priorytetem.

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Literatura

1. Ralph Langer
"Cracking Stuxnet, a 21st-century cyber weapon"
TED Talk 2011

http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html

2. Wikipedia: Stuxnet

http://pl.wikipedia.org/wiki/Stuxnet

3. Robert McMillan
„Stuxnet industrial worm written a year ago"
CSO Magazine

http://www.csoonline.com/article/602165/stuxnet-industrial-worm-written-a-year-ago

4. Robert McMillan
„Iran was prime target of SCADA worm"
Computerworld

http://www.computerworld.com/s/article/9179618/Iran_was_prime_target_of_SCADA_worm

5. Nicolas Falliere, Liam O Murchu, Eric Chien, Symantec
"W32.Stuxnet Dossier"

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

6. David E.Sanger
"Obama Order Sped Up Wave of Cyberattacks Against Iran"

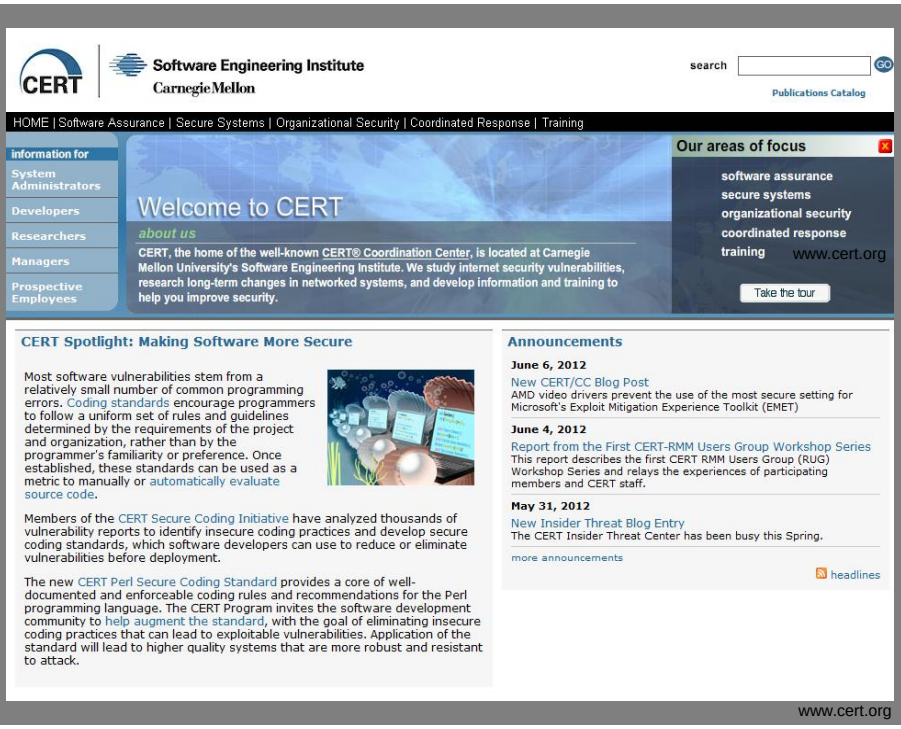
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all

Niniejszy artykuł jest pierwszym z serii artykułów dotyczących zespołów CERT. W następnych publikacjach poruszane będą tematy polskiego środowiska CERT-owego, zasad tworzenia CERT-ów, zasad ich funkcjonowania, używanych narzędzi, współpracy krajowej i międzynarodowej.

CERT historia powstania i zakres działania

JAK POWSTAŁA IDEA CERT-owa?

Aby zrozumieć to kiedy i w jakich okolicznościach powstała idea CERT (Computer Emergency Response Team) warto sobie wyobrazić następującą sytuację. Jest początek listopada 1988 roku. Kilka dni wcześniej - 2 listopada, w sieci pojawił się groźny wirus, który w historii zagrożeń internetowych nazywany jest Internet Worm lub Morris Worm. Odpowiedzialnym za wirusa był młody informatyk z Uniwersytetu Cornell – Robert Morris, notabene syn szefa informatyków amerykańskiej Państwowej Agencji Bezpieczeństwa (National Security Agency). Poprzez błąd w oprogramowaniu, polegający na nieprawidłowo wprowadzonych ograniczeniach propagacji, wirus w krótkim czasie sparaliżował ówczesny Internet, zarażając około 6 tysięcy komputerów. Na uniwersytecie Carnegie Mellon w Pittsburghu spotykają się specjaliści, którzy chcą się zastanowić nad zaistniałą sytuacją. Przypadek Morris Worma uświadamia im, jak podatny może być Internet na poważne zagrożenia, niezależnie od tego czy działanie wywołujące zagrożenie spowodowane zostało działaniem umyślnym czy nie. Dochodzą do wniosku, że w przyszłości na takie sytuacje warto być dobrze przygotowanym i móc jak najszybciej reagować i jak najskuteczniej ograniczać negatywne skutki zaistniałego zagrożenia. Dlatego decydują, aby powołać do życia zespół reagowania na przypadki naruszania bezpieczeństwa komputerowego – Computer Emergency Response Team, w skrócie CERT. Dwa tygodnie po pojawieniu się Morris Worma powstaje CERT/CC (CERT Coordination Center). Twórcy tej inicjatywy zapewne nie zdawali sobie sprawy z tego, że właśnie doprowadzili do pojawienia się tworu, który od tej pory będzie postrzegany jako jedna z najbardziej skutecznych metod nie tylko na reagowanie na incydenty, ale w ogóle dbania o odpowiedni poziom bezpieczeństwa w swoim obszarze działania, powszechnie określanym jako „*constituency*". Koncepcja się sprawdziła. Dziś na świecie istnieje kilkaset zespołów CERT-owych, a ponad 200 z nich jest zgromadzonych w międzynarodowej organizacji FIRST (Forum of Incident Response and Security Teams). Działają one w najróżniejszych środowiskach.



www.cert.org

CZYM WŁAŚCIWIE ZAJMUJĄ SIĘ CERT-y?

To, czym zajmują się CERT-y, w dużym stopniu wyjaśnione jest poprzez samą nazwę, którą najczęściej tłumaczy się na Zespół Reagownia na Przypadki Naruszenia Bezpieczeństwa Teleinformatycznego. Krótko mówiąc zespoły CERT-owe rozpoczynają swoją działalność przede wszystkim wtedy, kiedy dojdzie już do skutecznego ataku teleinformatycznego. Takie są przynajmniej założenia podstawowe, w praktyce ten zakres działalności wygląda znacznie szerzej. Jeśli spojrzymy na listę usług[1], opublikowanych przez wspomniany amerykański CERT Coordination Center, które świadczą CERT-y jest ich znacznie więcej. Rzecz jasna najważniejszymi usługami są właśnie **usługi reaktywne**. Wśród nich, oprócz wspomnianego już reagowania na incydenty, są jeszcze usługi obsługi słabości systemowych i analizy oprogramowania pod względem jego podatności na różne ataki komputerowe. Oprócz usług reaktywnych są jeszcze usługi **proaktywne** i te, które określane są usługami zarządzania bezpieczeństwem. Proaktywne usługi stają się coraz ważniejsze dla CERT-ów. Polegają one przede wszystkim na wnikliwej obserwacji świata zagrożeń teleinformatycznych i podejmowaniu akcji wynikających z ich pojawienia się, czyli na przykład ostrzegania członków swojego *constituency*. To niezwykle ważna usługa. Przy olbrzymiej skali obecnych zagrożeń dotarcie do każdej informacji, mogącej mieć wpływ

[1] CSIRT Services: http://www.cert.org/csirts/services.html

na bezpieczeństwo nie jest łatwe, nie tylko dla indywidualnych użytkowników sieci, ale nawet dla organizacji, które posiadają swoje własne zespoły bezpieczeństwa. Chodzi przede wszystkim o prawidłową ocenę ważności tej informacji. Bez codziennej praktyki w realizacji tego zadania jest to przedsięwzięcie bardzo trudne.

Najpowszechniejsza metoda monitorowania sieci i wyłapywania najgroźniejszych sytuacji działania polega na wykorzystaniu systemów typu IDS (Intrusion Detection System). Zespoły CERT-owe rozwijają na swoje potrzeby tego typu systemy. Ale robią jeszcze dodatkową rzecz, która jest niezwykle skuteczna. Otóż na bieżąco wymieniają się informacją na temat zagrożeń we własnej sieci. Te informacje dotyczą zarówno nowych zaobserwowanych metod ataków, jak również konkretnych zaatakowanych komputerów w sieci. Jeśli jeden zespół CERT-owy, monitorując bezpieczeństwo swoich klientów[1], napotka na ślady ataków na klientów innego zespołu CERT-owego, to może przekazać te informacje właśnie do tego innego CERT-u. Tak często się dzieje. CERT-y czy to w trybie ad hoc, czy w sposób systematyczny, przy wsparciu narzędzi technicznych, wymieniają się tego typu danymi. Dzięki temu informacje o zagrożeniach mogą trafić bardzo szybko do najbardziej zainteresowanego adresata, czyli po prostu do ofiary ataku. W sytuacji kiedy masa ataków sieciowych nie jest w ogóle zauważana przez użytkowników sieci, to jest to działanie bardzo ważne i pożyteczne.

Kolejną istotną usługą CERT-ową jest prowadzenie działań uświadamiających i szkoleniowych. CERT-y organizują szkolenia i warsztaty, jak również duże konferencje. Publikują również materiały uświadamiające, dotyczące zarówno podstawowych aspektów bezpieczeństwa jak i bardziej wyrafinowanych zagadnień. Jest to systematyczna praca u podstaw. Doświadczenia w edukacji tzw. „zwykłego Internauty" wykazały jednak, zdaniem wielu specjalistów, że takie podstawowe działania edukacyjne w niewielkim stopniu zmieniają zachowania Internautów, którzy ciągle popełniają te same proste błędy, prowadzące do poważnych konsekwencji. Jednak nie jest to do końca prawdą. Po prostu nie można założyć stuprocentowej skuteczności takiej działalności. Obserwacja prostych błędów może być frustrująca, ale nie zmienia to faktu, że takie działania uświadamiające dokonały już wielu pozytywnych zmian w zachowaniu Internautów i nie należy ich porzucać.

CZY WARTO MIEĆ SWÓJ CERT?

Niektórych może zdziwić tak postawione pytanie. Jak to? Swój CERT? To można mieć swój CERT? Otóż tak – można i nawet warto. Przez lata funkcjonował w Polsce mit, i chyba nadal w niektórych środowiskach funkcjonuje, że CERT to rzecz ekskluzywna i nie każdy ma w ogóle prawo takowy powoływać. Nieraz w prasie można było przeczytać informację o pierwszym polskim CERT-cie – CERT Polska, że jest filią CERT-u amerykańskiego. Nie ma czegoś takiego. Każdy CERT jest oddzielną, niezależną od drugiego CERT-u jednostką. Działają one w różnych środowiskach i na różnych poziomach. Owszem są CERT-y rządowe czy narodowe, ale są też CERT-y dla poszczególnych firm czy organizacji. W Polsce jest to CERT Pionier, działający na rzecz bezpieczeństwa w sieci Pionier, TP-CERT dla sieci firmy Orange, czy CSIRT Alior Bank, czyli pierwszy polski CERT powołany dla instytucji bankowej. Krótko mówiąc, CERT może powołać każdy. Oczywiście naturalne jest, że wcześniej powstanie on w dużej organizacji, w szczególności takiej, która ma potrzebę reagowania na incydenty. Nie znaczy to jednak, że inne organizacje nie mają prawa i możliwości tworzenia swoich CERT-ów. Warto nad tym się zastanowić i przemyśleć zalety i wady takiej decyzji. Nasz cykl artykułów ma za cel pomóc w takiej decyzji.

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

[1] termin klient w tym przypadku może być rozumiany zarówno komercyjnie, jak również niekomercyjnie, wtedy kiedy opisuje korzystającego z usług CERT-u.

Infrastruktura krytyczna to termin nadużywany

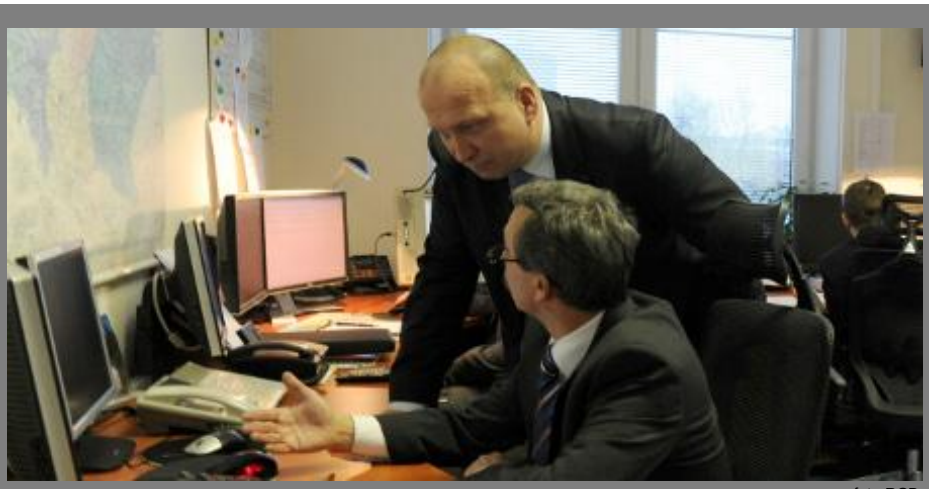


foto RCB

Dyrektor Rządowego Centrum Bezpieczeństwa Marek Komorowski o cyberprzestrzeni, infrastrukturze krytycznej, sposobach i programach jej ochrony, a także o istocie współpracy i wzajemnym zaufaniu.

CIIP focus: - Panie Dyrektorze, co łączy Rządowe Centrum Bezpieczeństwa z zagrożeniami cyberprzestrzeni i jej ochroną?

Marek Komorowski: - Z zagrożeniami absolutnie nic! Rolą RCB jest koordynacja działań z zakresu zarządzania kryzysowego i ochrony infrastruktury krytycznej. Zdarzenie zaistniałe w cyberprzestrzeni może być powodem sytuacji kryzysowej i zagrożeniem dla sprawnego funkcjonowania infrastruktury krytycznej.

- **Zarządzanie kryzysowe, infrastruktura krytyczna to terminy dość często i powszechnie występujące w dyskusji na tematy bezpieczeństwa, obronności…**

- Często są nadużywane. Niejednokrotnie zdarza się, że interlokutorzy chcąc podkreślić wagę swoich wypowiedzi, odwołują się do tych terminów. Prowadzi to do wielu nieporozumień. A pamiętać warto, że definicje infrastruktury krytycznej, jej ochrony, sytuacji kryzysowej są ujęte w ustawie o zarządzaniu kryzysowym.

- **Który z tych terminów „cierpi" najbardziej?**

- Zdecydowanie infrastruktura krytyczna. Używając terminu *infrastruktura krytyczna*, powinniśmy być świadomi, że mówimy o konkretnych obiektach, urządzeniach, instalacjach czy usługach, które są wymienione w *wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej*. Wykaz ten jest niejawny, więc dostęp do niego jest ograniczony, stąd co najmniej niefortunne są wypowiedzi wielu ekspertów, którzy w szczegółach rozprawiają o infrastrukturze krytycznej.

- **Ale przyzna Pan, że o charakterystyce infrastruktury krytycznej można wiele wnioskować na podstawie ustawy. Definicja IK obejmuje przykładowo system sieci teleinformatycznych i system łączności.**

- Ustawodawca określił 11 obszarów, które są istotne dla sprawnego funkcjonowania społeczeństwa i państwa, nazywając je systemami. Takim podejściem kierowano się również przy wyznaczaniu, a także ochronie infrastruktury krytycznej. Rozwiązania zastosowane w Polsce występują również w innych krajach, które stworzyły, bądź tworzą, system ochrony własnej IK. W USA, Wielkiej Brytanii, Holandii, Francji oraz w Niemczech także możemy zaobserwować podział na sektory krytyczne dla funkcjonowania państwa, społeczeństwa i gospodarki. Właściciel lub operator IK został tam także uznany jako odpowiedzialny za jej ochronę, a organy administracji odpowiadają za koordynację działań w danym sektorze.

- **Jak zatem wyznacza się konkretną infrastrukturę, o której Pan wspominał, tę znajdującą się w wykazie?**

- Należy odwołać się do kryteriów. Są ich dwa rodzaje. Pierwszy z nich to kryteria systemowe, opisujące cechy charaktery-

Definicje zawarte w ustawie o zarządzaniu kryzysowym:

Zarządzanie kryzysowe - działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej.

Sytuacja kryzysowa - sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.

Infrastruktura krytyczna - systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Ochrona infrastruktury krytycznej - wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

styczne dla obiektów w danym systemie. Tam, gdzie to możliwe, cechy te przedstawiono w postaci liczbowej np. średnica rurociągu. Drugi rodzaj to kryteria przekrojowe, wspólne dla wszystkich systemów. Opisują one skutki zakłócenia funkcjonowania infrastruktury: ile osób zostanie poszkodowanych, jakie będą straty ekonomiczne itp. Metodyka przewiduje, że infrastruktura wyłoniona w drodze spełnienia kryteriów systemowych jest porównywana z definicją infrastruktury krytycznej zawartą w ustawie. Ten etap selekcji jest ważny, ponieważ pozwala zaoszczędzić wiele pracy w ostatnim etapie – szacowaniu skutków zakłócenia funkcjonowania infrastruktury.

- **Opracowanie obu rodzajów kryteriów musiało stanowić wyzwanie…**

- Owszem. Tym bardziej, że ustawodawca w przepisach przejściowych do nowelizacji ustawy o zarządzaniu kryzysowym wskazał ambitny termin ich opracowania. W RCB zorganizowaliśmy cykl spotkań z podmiotami reprezentującymi dany system. Przedstawiliśmy im nasze propozycje i skonfrontowaliśmy je z ich opiniami. Następnie, we współpracy z właściwymi ministrami i kierownikami urzędów centralnych, została opracowana obowiązująca wersja kryteriów. Pamiętajmy jednak, że kryteria nie zostały jednak ustalone raz na zawsze. W razie potrzeby można dokonać ich aktualizacji. Ponadto, warto uświadomić sobie, że żyjemy w czasach dynamicznych zmian. Technologia komputerowa jest tego najlepszym przykładem. Trudno jest zatem wskazać ponadczasowe i uniwersalne kryteria. Zresztą w odniesieniu do systemów łączności i sieci teleinformatycznych opracowanie kryteriów to wyzwanie nie tylko na poziomie krajowym, ale i europejskim.

- **To oznacza, że temat infrastruktury krytycznej jest obecny w Brukseli?**

- Tak, zajmuje się tą kwestią Generalna Dyrekcja do Spraw Wewnętrznych Komisji Europejskiej. Przy współpracy państw członkowskich, opracowano Europejski Program Ochrony Infrastruktury Krytycznej (EPOIK) stanowiący komunikat Komisji Europejskiej. W ramach tego Programu przyjęto dyrektywę (Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. – przyp. red.), na podstawie której wyznaczono europejską infrastrukturę krytyczną. W tej chwili trwa przegląd polityki odnoszącej się do IK, którego efekty poznamy pod koniec roku. W obszarze ochrony IK Rządowe Centrum Bezpieczeństwa jest dla Komisji punktem kontaktowym.

- **Czym europejska infrastruktura różni się od krajowej?**

- Jak na razie państwa członkowskie zgodziły się, że wyznaczą IK tylko w sektorach energetycznym i transportowym. Obiekty zostają zakwalifikowane jako krytyczne tylko wówczas, jeśli zakłócenie funkcjonowania odpowiedniej infrastruktury będzie odczuwalne w co najmniej dwóch państwach członkowskich UE.

- **Czyli sektor technologii teleinformacyjno-komunikacyjnych nie należy do europejskiej infrastruktury krytycznej?**

- Trwają dyskusje czy, a jeśli tak to w jaki sposób, dodać ten element do obszaru zainteresowania EPOIK czy Dyrektywy. Mówimy o najbardziej dynamicznie rozwijającym się sektorze, podczas gdy działania w ramach EPOIK są raczej powolne.

- **Wróćmy do problemu bezpieczeństwa w cyberprzestrzeni. Jak RCB może być pomocne przy jego zwiększaniu?**

- Kilkoma sposobami. Po pierwsze, wyznaczyliśmy infrastrukturę krytyczną w systemie sieci teleinformatycznych i w systemie łączności. Mamy więc skonkretyzowane potencjalne słabe punkty naszej cyberprzestrzeni. Na właścicielach IK ciąży obowiązek jej ochrony, przy czym tę ochronę rozumiemy szeroko, nie tylko jako ochronę fizyczną. Po drugie, w Narodowym Programie Ochrony Infrastruktury Krytycznej (dalej: „NPOIK" – przyp. red.) będzie można zapoznać się z szeregiem dobrych praktyk, które powinny pomóc stworzyć lepsze warunki do ochrony tej infrastruktury. W NPOIK proponujemy także podzielenie ochrony infrastruktury krytycznej na sześć obszarów. Obok ochrony fizycznej, technicznej, prawnej, osobowej i planów odbudowy koncentrujemy się także na ochronie teleinformatycznej. Po trzecie, angażujemy się w próby „uregulowania" cyberprzestrzeni, pozostawiając z boku dylemat, czy takie „uregulowanie" jest w ogóle możliwe. Pracownicy RCB brali czynny udział w opracowaniu projektu Polityki Bezpieczeństwa Cyberprzestrzeni RP. Ponadto, w *Raporcie o zagrożeniach bezpieczeństwa narodowego* znalazła się ogólna charakterystyka zagrożeń cyberprzestrzeni, a w *Krajowym Planie Zarządzania Kryzysowego* zostały wskazane podmioty odpowiedzialne za koordynację działań w przypadku cyberataku oraz monitorowanie zagrożeń teleinformatycznych dla systemów administracji publicznej. Po czwarte, współpracujemy ze wszystkimi, którzy chcą poprawić poziom bezpieczeństwa w cyberprzestrzeni.

- **Współpracująca administracja? Rzadko spotykane, przynajmniej zdaniem wielu osób! Czy mógłby nam Pan trochę przybliżyć ten fenomen?**

- Administracja charakteryzuje się dużą bezwładnością, tak informacyjną, jak i decyzyjną – oczywiście to nie jest zarzut, taka po prostu jest jej cecha – nigdy nie będzie w stanie nadążyć za zmianami, zwłaszcza w tak dynamicznym obszarze jak cyberprzestrzeń. Dlatego skuteczne i działające rozwiązania z zakresu bezpieczeństwa pojawiają się najpierw u użytkowników systemów oraz sieci teleinformatycznych. Dobrym przykładem takich działań są zespoły CERT (*Computer Emergency Response Team* – Zespół Reagowania na Incydenty Komputerowe – przyp. red.), które pojawiły się spontanicznie w odpowiedzi na zapotrzebowanie użytkowników Internetu. Dopiero później w ten ruch włączyła się administracja. Polska jest jednym z krajów w których zespoły CERT działają poza sferą regulacji prawnych. I co najważniejsze, skutecznie działają! Innym pozytywnym przykładem są tzw. ISAC (*Information Sharing and Analisis Center* – Centrum Wymiany i Analizy Informacji – przyp. red.) organizowane np. przez przedsiębiorstwa z danego sektora gospodarki. W RCB próbujemy „wyłowić" te i inne ciekawe inicjatywy sprzyjające współpracy i „przenieść" je w polską rzeczywistość. Skuteczność współpracy na rzecz bezpieczeństwa cyberprzestrzeni uważam za najefektywniejszą i najbardziej przyszłościową formę walki z zagrożeniami. Dlatego m.in. zaangażowaliśmy się w inicjatywę znaną jako tzw. ROCK – Rok Ochrony Cyberprzestrzeni Krytycznej. Pracownicy RCB są częścią zespołu planistycznego ćwiczeń z zakresu ochrony cyberprzestrzeni oraz uczestniczą w konwersatoriach „Pięć żywiołów". Oba te przedsięwzięcia są częścią ROCKu. Współorganizujemy lub patronujemy konferencjom z zakresu cyberbezpieczeństwa. Przykładem może być np. konferencja „Ochrona Teleinformatyczna IK", która została zorganizowana wspólnie ze

spółką Polskie Sieci Energetyczne „Operator" (sprawozdanie z konferencji w dalszej części numeru – przyp. red.) lub konferencja „Bezpieczeństwo energetyczne państwa, a infrastruktura krytyczna", którą organizowały Polskie Górnictwo Naftowe i Gazownictwo SA oraz Operator Gazociągów Przesyłowych „Gaz-System" SA przy naszym udziale. Patronujemy także konferencji „Wolność i bezpieczeństwo", organizowanej przez wydawcę pisma „Computerworld".

- **Zaskakująco dużo, jak na administrację…**

- W NPOIK współpraca jest traktowana jako jeden z filarów bezpieczeństwa IK. W dokumencie tym cały rozdział poświęcony jest właśnie organizacji współpracy pomiędzy zainteresowanymi stronami. Planujemy ponadto utworzenie internetowej platformy służącej wymianie informacji.

- Co jeszcze powinno zwracać naszą szczególną uwagę w Narodowym Programie Ochrony Infrastruktury Krytycznej?

- Biorąc pod uwagę polską specyfikę i kulturę prawną, nasz system ochrony IK przewiduje rozwiązania regulacyjne, tzn. w przepisach prawa powszechnie obowiązującego literalnie wskazano na obowiązek ochrony IK przez jej właścicieli oraz posiadaczy samoistnych i zależnych, a także na konieczność sporządzenia planu ochrony i wyznaczenia osoby do kontaktów z administracją. Nakładając jednak na właściciela IK obowiązek ochrony, nie przewiduje się sankcji za jego niedopełnienie, aczkolwiek brak sankcji nie może oznaczać braku odpowiedzialności. Właściciele oraz posiadacze samoistni i zależni, którzy świadomie niedopełniają obowiązku ochrony infrastruktury krytycznej, narażają pracowników i innych ludzi na bezpośrednie niebezpieczeństwo utraty życia albo ciężkiego uszczerbku na zdrowiu, mogące być skutkiem zakłócenia funkcjonowania IK, a to z kolei jest zagrożone karą pozbawienia wolności do lat 3. Opracowując koncepcję Programu przyjęliśmy założenie, że chęć zachowania ciągłości biznesowej przez właściciela może być narzędziem skuteczniejszym w osiągnięciu wysokiego poziomu ochrony IK niż sankcja. W następstwie tego podejścia mniejsza jest niechęć wykonawców do realizacji zadań i mniej prób uchylania się od wypełniania obowiązków. Ponadto założyliśmy, że w działania z zakresu ochrony IK w większym stopniu należy zaangażować podmioty, które nią zarządzają - nie jednak w drodze nakazów i sankcji, ale świadomego udziału w przedsięwzięciu mającym na celu poprawę bezpieczeństwa systemów istotnych dla funkcjonowania społeczeństwa. W tym kontekście ważna jest też intensywna współpraca sektora prywatnego i publicznego. Doświadczenia innych krajów pokazują, że system oparty na dobrowolnym lub częściowo dobrowolnym uczestnictwie w ochronie IK działa skutecznie. Właściciele lub operatorzy IK, będąc częścią infrastruktury krytycznej, często sami domagają się uczestnictwa w takim systemie, co wiąże się dla nich z dostępem do informacji o zagrożeniach bezpieczeństwa przekazywanych przez administrację, wsparciem merytorycznym, a w sytuacji kryzysowej priorytetowym wsparciem siłami i środkami pozostającymi w dyspozycji władz. Obie strony: biznesowa i rządowa muszą jednak wykazać dojrzałość i świadomość współodpowiedzialności za poprawne funkcjonowanie IK.

- **Jak zatem układa się współpraca z sektorem prywatnym? W Polsce zaufanie do administracji rządowej jest chyba niewielkie.**

- Czynimy postępy, w szczególności jeżeli chodzi o infrastrukturę krytyczną. Współpracę z sektorem prywatnym traktujemy priorytetowo. Zdajemy sobie sprawę, że to sektor prywatny dysponuje najlepszymi ekspertami, jest w stanie podzielić się najefektywniejszymi praktykami i swoim bezcennym doświadczeniem. My chcemy stworzyć takie warunki, które pozwolą operatorom na wymianę doświadczeń. Im pozwoli to na efektywne działanie i oszczędzenie środków, a administracja będzie mogła podnieść poziom odporności funkcjonowania państwa na różnorakie zagrożenia.

- **Nakreślił Pan podstawowe założenia NPOIK. A zasady, na których Program się opiera?**

- NPOIK w sposób syntetyczny i kompleksowy przedstawia wizję, cele i standardy ochrony IK oraz sposób współpracy w realizacji zadań. NPOIK opiera się na trzech filarach. Są to: po pierwsze - współodpowiedzialność – jako wiodąca zasada przyjęta przy budowie systemu ochrony infrastruktury krytycznej. Rozumiana jest jako wspólne, zbiorowe dążenie do poprawy bezpieczeństwa IK, wynikające ze świadomości znaczenia tego segmentu dla funkcjonowania nie tylko organów administracji publicznej i operatorów IK, lecz wręcz społeczeństwa, gospodarki i w konsekwencji – państwa. Drugim filarem jest współpraca, o której już wspominałem. Oznacza wykonywanie razem przez uczestników ochrony IK określonych, zbieżnych i wzajemnie uzupełniających się zadań dla osiągnięcia wspólnego celu. Współpraca jest niezbędna, skoro chce się uniknąć duplikacji działań i niepotrzebnych kosztów oraz efektywniejszego wykorzystania posiadanych sił i środków. Warunkiem skutecznej współpracy jest jej autentyczność, wzajemność i dążenie do wspólnej korzyści. Ostatnim filarem jest zaufanie rozumiane jako przekonanie, że motywacją działania uczestników ochrony IK, dotyczy to w szczególności administracji i operatorów IK, jest wspólny cel, czyli poprawa bezpieczeństwa IK. W NPOIK jest ujętych jeszcze kilka innych zasad, ale jest to temat na kolejną rozmowę (w następnych numerach postaramy się przybliżyć najważniejsze elementy NPOIK – przyp. red.). NPOIK jest wyjątkowy również dlatego, że w nowatorski i kompleksowy sposób podchodzi do zagadnienia bezpieczeństwa, m.in. więcej miejsca poświęca edukacji i potrzebie zaangażowania w bezpieczeństwo IK świata nauki oraz całego społeczeństwa.

- Kiedy zatem Program zostanie oficjalnie przyjęty?

- Mam nadzieję, że wkrótce uda nam się osiągnąć porozumienie ze wszystkimi, którzy są w niego zaangażowani.

- I tego życzmy. Dziękuję za rozmowę.

Ochrona Teleinformatyczna Infrastruktury Krytycznej

Ochrona teleinformatyczna, potencjalne skutki cyberataków oraz zależność sektora energetycznego od systemów teleinformatycznych, to tylko niektóre z tematów poruszanych przez uczestników konferencji „Ochrona Teleinformatyczna Infrastruktury Krytycznej", zorganizowanej przez Rządowe Centrum Bezpieczeństwa (RCB) oraz Polskie Siecie Elektroenergetyczne Operator SA. Konferencja odbyła się 26 kwietnia 2012 r. w siedzibie spółki PSE Operator SA w Konstancinie - Jeziornie.

Spotkanie otworzyli Marek Komorowski – dyrektor RCB oraz Kazimierz Kułaga – członek zarządu PSE Operator SA. Zdaniem obu coraz większe zastosowanie w procesach przemysłowych oraz codziennym życiu technologii teleinformatyczno-komunikacyjnych powoduje, że zagrożenia pochodzące z cyberprzestrzeni stają się jednymi z bardziej powszechnych i realnych zagrożeń dzisiejszych czasów. Ochrona teleinformatyczna stanowi jeden z filarów bezpieczeństwa organizacji. Ma ona szczególne znaczenie w odniesieniu do najważniejszych w państwie obiektów, instalacji, urządzeń i usług. W związku z tym, powinna stać na wysokim poziomie i być traktowana na równi z innymi rodzajami ochrony np. ochroną fizyczną. Ponieważ zrozumienie zagrożeń jest niezwykle istotne do podjęcia efektywnych działań ochronnych, organizatorzy zaprosili przedstawicieli sektora energetycznego, a także Ministerstwa Gospodarki oraz Ministerstwa Skarbu Państwa, aby omówić problematykę związaną z ochroną teleinformatyczną, uświadomić uczestnikom podatności systemów teleinformatycznych na zagrożenia, pokazać potencjalne skutków cyberataków, przedstawić zależność sektora energetycznego od systemów teleinformatycznych, pokazać sposoby reakcji na incydenty komputerowe oraz usystematyzować wiedzę i podejście do ochrony teleinformatycznej.

Aby osiągnąć zakładane cele, organizatorzy poprosili o prelekcję przedstawicieli: Naukowej i Akademickiej Sieci Komputerowej (NASK), CERT Polska (*Computer Emergency Response Team* – zespół reagowania na zagrożenia i incydenty w sieciach komputerowych), CERT.GOV.PL Agencji Bezpieczeństwa Wewnętrznego, Systemu Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej (SRnIK RON), Fundacji Bezpieczna Cyberprzestrzeń (FBC) oraz reprezentantów spółek Gaz-System SA i PSE Operator SA.

Piotr Kijewski – kierownik zespołu CERT Polska przedstawił najważniejsze dane z raportu nt. bezpieczeństwa sieciowego, sporządzonego na podstawie incydentów zgłoszonych do CERT Polska. Zaprezentował także system wczesnego wykrywania i ostrzegania o zagrożeniach ARAKIS, bazujący na rozwiązaniach typu honeypot. Następnie przedstawiciel CERT Polska omówił możliwości wczesnego ostrzegania o zagrożeniach w sieciach teleinformatycznych oraz zaprezentował uczestnikom autorską platformę n6. Służy ona do wymiany informacji o zagrożeniach i incydentach.

Dzięki prezentacji Krzysztofa Silickiego – dyrektora technicznego NASK – uczestnicy konferencji mieli okazję zapoznać się z aktualnymi inicjatywami w dziedzinie bezpieczeństwa teleinformatycznego w Polsce i na świecie. Dyrektor Silicki przekonywał, że współpraca pomiędzy zainteresowanymi stronami w przypadku zagrożeń z cyberprzestrzeni może być wyjątkowo skuteczna. Na poparcie swych słów przedstawiciel NASK zapoznał uczestników z inicjatywami i efektami prac Komisji Europejskiej, Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), z inicjatywą FIRST (Forum of Incident Response and Security Teams) oraz przykładami ćwiczeń Cyber Europe 2010 oraz Baltic Cybershield.

foto RCB

Marek Komorowski
Dyrektor Rządowego Centrum Bezpieczeństwa

Rządowy zespół reagowania na incydenty komputerowe CERT.GOV.PL przedstawił zebranym cele swojego działania, zaprezentował narzędzia wykorzystywane w pracy, tj. system ARAKIS-GOV oraz HoneySpider Network-GOV oraz omówił, jakie zagrożenia dla infrastruktury krytycznej identyfikowane są obecnie jako najważniejsze.

foto RCB

Kazimierz Kułaga
Członek Zarządu PSE Operator S.A.

PSE Operator SA reprezentował Tadeusz Włodarczyk – starszy specjalista w Departamencie Teleinformatyki Sekcji Bezpieczeństwa i Standardów IT. W swojej prezentacji przedstawił praktyczne zagadnienia związane z wdrażaniem normy ISO 27001 do ochrony teleinformatycznej infrastruktury krytycznej Spółki. Przedstawiciel PSE Operator SA wskazał równocześnie przykłady incydentów bezpieczeństwa w systemach SCADA, którym można byłoby zapobiec, stosując się do wdrożonych polityk bezpieczeństwa.

Michał Kraut ekspert ds. bezpieczeństwa sieciowego, zapoznał uczestników

foto RCB

Uczestnikami konferencji byli przedstawiciele Ministerstw Gospodarki oraz Skarbu Państwa, a także prezesi oraz pracownicy firm zarządzających kluczową dla bezpieczeństwa państwa infrastrukturą.

z implementacją w systemach i sieciach zasad bezpieczeństwa określonych w politykach bezpieczeństwa, ze szczególnym uwzględnieniem modelowych architektur sieci SCADA i systemów dostępu do nich.

Przedstawiciel SRnIK RON – Marcin Brzeziński – omówił zagadnienia bezpieczeństwa w kontekście realizowanych przez siebie zadań związanych z ochroną systemów rozproszonych. Przedstawiona została charakterystyka systemów rozproszonych oraz zagrożenia wewnętrzne i zewnętrzne dla takiej struktury, jakie mogą spotkać na swej drodze przedsiębiorstwa budujące systemy ochrony sieci rozproszonych. Jako prawdziwe wyzwanie przedstawiciel MON wskazał ochronę systemów rozproszonych o różnych klauzulach (jawnych i niejawnych). Marcin Brzeziński podkreślił, że nie tylko działania techniczne mają znaczenie dla bezpieczeństwa teleinformatycznego. Równie ważne są działania edukacyjne oraz dbałość o personel.

Michał Pawlak i Kamil Kowalczuk z GAZ-System SA przedstawili uczestnikom konferencji swoje doświadczenia w zakresie ochrony rozproszonych systemów SCADA i na ich przykładzie omówili wysoki stopień zależności funkcjonowania systemów infrastruktury krytycznej od sprawnego funkcjonowania sieci i systemów teleinformatycznych. Przedstawili także sposoby zapobiegania skutkom awarii systemów ICT.

Mirosław Maj z Fundacji Bezpieczna Cyberprzestrzeń (FBC) przekazał informacje na temat standardów i dobrych praktyk w zakresie ochrony teleinformatycznej. O tym, że zagrożenia z cyberprzestrzeni nie są „wirtualne" przedstawiciel FBC przekonywał zebranych pokazując szereg przykładów incydentów bezpieczeństwa w systemach infrastruktury krytycznej. Na koniec zaprosił do uczestnictwa w konferencji "Wolność i Bezpieczeństwo 2012", w ramach której zostaną przeprowadzone pierwsze w Polsce ćwiczenia reagowania na cyberataki. Warte podkreślenia jest, że ćwiczenia organizowane są jako inicjatywa podmiotów spoza administracji, która przyjęła na siebie rolę wspomagającą.

Konferencję zakończyła dyskusja panelowa. Zabierający głos przedstawiciele sektora energetycznego wskazywali przede wszystkim na potrzebę zwiększenia koordynacji działań w zakresie ochrony przed zagrożeniami z cyberprzestrzeni. Ich zdaniem to administracja powinna zapewnić dostęp do informacji o zagrożeniach oraz podejmować kroki zaradcze w przypadku wystąpienia cyberataków. Na drugim biegunie znajdowały się opinie, iż to sami przedsiębiorcy w główniej mierze są odpowiedzialni za ochronę swojego biznesu, w związku z czym nie mogą czekać na reakcję ze strony władz. Przedstawiciele RCB wskazywali natomiast, że obydwa podejścia można i należy zastosować jednocześnie. Problemem pozostają właściwe proporcje. Pokazali dla przykładu, jak te proporcje mogłyby się układać: monitoring i informowanie o zagrożeniach – administracja, ochrona i minimalizacja skutków potencjalnego cyberataku – właściciele infrastruktury.

Konferencję zamknął zastępca dyrektora RCB Kamil Galicki, wskazując na potrzebę kontynuacji dialogu o ochronie teleinformatycznej oraz organizacji podobnych konferencji. Dyr. Galicki podkreślił również konieczność współpracy, jako wyjątkowo skutecznego sposobu radzenia sobie z nowymi zagrożeniami pochodzącymi z cyberprzestrzeni.

Maciej Pyznar
Wydział Ochrony Infrastruktury Krytycznej RCB

Tadeusz Włodarczyk
PSE Operator SA

Od Redakcji: Ponieważ podczas konferencji poruszono wiele ciekawych wątków, które z pewnością zainteresują szersze grono czytelników, poprosiliśmy prelegentów o rozwinięcie niektórych z nich. Postaramy się zapoznać Państwa z otrzymanymi materiałami w jednym z najbliższych numerów.

Następny numer „CIIP focus" ukaże się pod koniec sierpnia.

Zachęcamy do kontaktu z redakcją "CIIP focus".