Nr 3 - Grudzień 2012

CIIP focus

RCB
Rządowe Centrum Bezpieczeństwa

foto IDG

Ćwiczenia, ćwiczenia ...i po ćwiczeniach

CYBER-EXE POLSKA 2012

19 września we wrocławskiej Hali Stulecia odbyło się pierwsze w Polsce ćwiczenie z ochrony teleinformatycznej strategicznej dla funkcjonowania państwa infrastruktury. Krótkie podsumowanie i pierwsze wnioski, jakie pojawiły się zaraz po jego zakończeniu - str. 3

CYBER EUROPE 2012

Na początku października Europejska Agencja Bezpieczeństwa Sieci i Informacji przeprowadziła drugie ogólnoeuropejskie ćwiczenie z ochrony cyberprzestrzeni. Cele, przebieg i inne interesujące informacje w relacji naszego korespondenta - s. 6

W NUMERZE:

Drodzy Czytelnicy,

To już trzeci numer naszego magazynu. Wszystko wskazuje na to, że będą kolejne, ponieważ jak na razie nie ma powodów aby było inaczej. Nawet przeciwnie. Docierają do nas głosy z pochwałami i gratulacjami, nie tylko za podjęcie inicjatywy, ale przede wszystkim za treść merytoryczną *CIIP focus*. Jedno i drugie bardzo cieszy. Dziękujemy. Z Państwa opinii wynika, że model rozwoju magazynu jaki został przyjęty sprawdza się. Staramy się opisywać najważniejsze wydarzenia w dziedzinie ochrony teleinformatycznej, w szczególności tej dotyczącej infrastruktury krytycznej. Mamy nadzieję, że trafiamy do osób i instytucji, którzy w sposób ciekawy opisują zagadnienia z zakresu tematyki magazynu.

Dominującym tematem pierwszych trzech numerów magazynu stało się ćwiczenie Cyber-EXE Polska 2012, które miało swój finał operacyjny we wrześniu we Wrocławiu. Formalny finał ćwiczenia odbędzie się 19 grudnia w trakcie seminarium zorganizowanego w Stowarzyszeniu Euro-Atlantyckim, podczas którego przedstawiony zostanie raport końcowy z ćwiczenia. Warto podkreślić, że raport ten zaprezentują dwaj nasi stali autorzy, czyli Maciej Pyznar z RCB i Mirosław Maj z FBC, którzy o ćwiczeniach, polskich i europejskich, piszą również w tym numerze. Ta częstotliwość poruszania tego tematu nie jest przypadkowa. Było to naprawdę duże przedsięwzięcie. Materiał i doświadczenia jakie zostały zebrane przy okazji Cyber-EXE Polska 2012 starczyłby jeszcze na kilka numerów, jednak zadbamy o to, aby nie zanudzić naszych czytelników tym tematem. Zresztą i w tym numerze znajdą Państwo artykuły z innej tematyki.

Kamil Kowalczuk z Gaz-System SA opowiada swoją historię z systemami SCADA i dzieli się praktyczną wiedzą na temat tego, jak zapewnić bezpieczeństwo tych systemów. Jeśli ktoś stworzy listę kontrolną zadań bezpieczeństwa dla SCADA na podstawie Jego artykułu, to zachęcamy do podzielnia się nią z redakcją.

W trzecim numerze poruszmy też tematy związane ze współpracą różnych środowisk w Polsce, które mają duży wpływ na bezpieczeństwo teleinformatyczne w naszym kraju. Mirosław Maj opisuje historię stworzenia i działanie Abuse-Forum, a wiceprezes Związku Banków Polskich - dr Mieczysław Groszek opowiada o tym, czym zajmuje się i jak funkcjonuje ZBP. Wspomina rzecz jasna również o tematyce bezpieczeństwa w środowisku bankowym.

Pierwsze dwa numery *CIIP focus* pobrano ponad 3 000 razy. W naszej redakcji nikt nie spodziewał się takiego zainteresowania. Bardzo za nie dziękujemy i zapewniamy, że to dla nas wspaniała motywacja do dalszej pracy.

Redakcja *CIIP focus*

NEWS

Po raz kolejny Amerykanie boją się cyfrowego Pearl Harbor – operacja „Szamun”

Scenariusz elektronicznego Pearl Harbor pojawia się w literaturze już od co najmniej kilkunastu lat. Po raz kolejny o tym zagrożeniu słyszymy przy okazji analizy dużego ataku, jaki miał miejsce w Arabii Saudyjskiej na największą firmę naftową świata – Saudi Aramco. W trakcie tego ataku przepadły dane z około 30 000 komputerów. Do ataku przyznała się organizacja „Miecz Sprawiedliwości”. Następnym celem ataku była katarska firma RasGas. Zdaniem specjalistów z Departamentu Obrony USA to demonstracja siły, ale również realne zagrożenie o potencjalnie katastrofalnych skutkach.

Więcej: http://bit.ly/QMrHK8

9 nowych słabości systemowych SCADA, które nie trafią do producentów

Maltańska firma specjalizująca się w wyszukiwaniu słabości systemowych poinformowała, że odnalazła 9 groźnych słabości systemowych SCADA takich producentów jak: General Electric, Schneider Electric, Kaskad, Rockwell Automation, Eaton and Siemens. Jednocześnie Maltańczycy poinformowali, że nie przekażą informacji o tych słabościach do producentów, natomiast liczą na to, że sprzedadzą je zainteresowanym rządom i użytkownikom systemów. Praktyka, jaką stosują odkrywcy słabości, jest nowością o tyle tylko, że dotychczas podobne praktyki miały miejsce przy zachowaniu dyskretności tego typu ataków. Systemy SCADA nadal są postrzegane jako te, których bezpieczeństwo jest na dość niskim poziomie, co przy znaczących konsekwencjach ich zaatakowania, stanowi nie lada zagrożenie.

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

Ćwiczenie Cyber - EXE Polska 2012

Podsumowanie i pierwsze wnioski

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Pierwsze polskie ćwiczenie z ochrony infrastruktury strategicznej dla funkcjonowania państwa jest już za nami. Mamy nadzieję, że 19 września we Wrocławiu, przy okazji IX edycji konferencji Wolność i Bezpieczeństwo, udało się zapoczątkować coś, co na stałe wejdzie do kalendarza najważniejszych wydarzeń z dziedziny bezpieczeństwa w cyberprzestrzeni w Polsce. Przygotowania, przebieg i pierwsze konkluzje po ćwiczeniu wskazują na to, że tak właśnie może się stać.

Jakąkolwiek opowieść o Cyber-EXE Polska 2012 trzeba koniecznie zacząć od stwierdzenia, że mieliśmy do czynienia z bardzo ważnym przypadkiem udanej współpracy pomiędzy administracją państwową i sektorem prywatnym. Nie zamierzam pisać laurki dla Cyber-EXE Polska 2012, bo było w tym ćwiczeniu również kilka rzeczy, które warto poprawić w następnych edycjach, a i na wspomnianej współpracy są pewne rysy, ale nie ma sensu też grzeszyć nadmierną skromnością i unikać stwierdzenia, że eksperyment okazał się udany. W jego wyniku powstał bardzo ciekawy materiał, którego dobra analiza może w istotny sposób wpłynąć na poprawę bezpieczeństwa cyberprzestrzeni w Polsce.

Dla porządku przypomnijmy kilka istotnych faktów dotyczących tego ćwiczenia. Jego organizatorem był Tygodnik Computerworld, Instytut Mikromakro i Fundacja Bezpieczna Cyberprzestrzeń. Ta ostatnia pełniła rolę koordynatora merytorycznego ćwiczenia. Warto jednak przy okazji organizacji wspomnieć o dwóch innych instytucjach. Jednej krajowej, a jednej europejskiej. Tą drugą była Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA), której materiały przygotowane po ćwiczeniu Cyber Europe 2010 posłużyły jako wzorzec metodyczny w przygotowaniu i przeprowadzeniu polskiego ćwiczenia. Sama zaś Agencja aktywnie włączyła się w przygotowania, organizując między innymi warsztaty przygotowawcze dla zespołu projektowego, które odbyły się w Warszawie. Natomiast instytucją krajową, o której trzeba wspomnieć jest Rządowe Centrum Bezpieczeństwa, które aktywnie włączyło się w realizację całej idei. Oprócz wspomnianych instytucji w ćwiczeniu wzięło udział wiele firm i organizacji. Nikt przy tej okazji nie powinien zostać pominięty, dlatego wymieńmy je wszystkie. Sektor publiczny, który uczestniczył w ćwiczeniu na warunkach dobrowolności i nieodpłatnie, reprezentowało obok RCB, Ministerstwo Obrony Narodowej i Komenda Główna Policji. Natomiast sektor prywatny to przedstawiciele Gaz-Systemu SA, PSE Operatora SA – głównych graczy w ćwiczeniu oraz RWE Polska SA i Orange Polska SA. Wszystko odbyło się przy dużym udziale specjalistów z Wojskowej Akademii Technicznej i wsparciu przedstawicieli Politechniki Wrocławskiej.

To tyle jeśli chodzi o listę zasłużonych. Warto teraz opowiedzieć o tym co działo się we Wrocławiu. 19 września o godzinie 9:00 rozpoczęło się całodzienne ćwiczenie. Ćwiczyliśmy tak naprawdę w dwóch warstwach – technicznej i organizacyjnej. Jeśli chodzi o tę pierwszą, to na potrzeby ćwiczenia zbudowane zostało środowisko testowe, w którym pojawiły się wirtualne wersje istotnych serwisów dla funkcjonowania systemu dystrybucji gazu. W tym środowisku miały miejsce ataki przeprowadzane przez „intruzów" (tzw. „red team"). Cały atak rozpoczął się od znanego w świecie cyberprzestrzeni ataku typu APT[1], dzięki któremu intruzi przedostali się do sieci korporacyjnej. Będąc w tejże sieci rozpoczę-

[1] Advanced Persistant Threat – http://en.wikipedia.org/wiki/Advanced_persistent_threat

NEWS

Ślady chińskich ataków na dostawcę urządzeń SCADA

Firma Televent, będąca producentem systemów kontroli i monitoringu procesów przemysłowych (tzw. SCADA), potwierdziła, że doświadczyła włamania do swojej sieci i kradzieży plików zawierających poufne informacje projektowe. Zdaniem producenta, sytuacja ta zwiększa niebezpieczeństwo skutecznego ataku na produkty Televent. Produkty Televent są odpowiedzialne za zarządzanie systemami, przez które przesyłane jest 140 00 GWh. Elektroniczne ślady przestępstwa prowadzą do chińskiej grupy hakerskiej zwanej „Comment Group". O zagrożeniu zostali poinformowani użytkownicy zagrożonych systemów. Więcej: http://bit.ly/P00Jiq

Firma Kaspersky pracuje nad bezpiecznym systemem operacyjnym dla systemów SCADA

Znana rosyjska firma antywirusowa – Kaspersky Lab – pracuje nad bezpiecznym systemem operacyjnym, który znalazłby zastosowanie w obsłudze systemów kontroli i monitoringu procesów przemysłowych (tzw. SCADA). System powstaje w odpowiedzi na coraz częściej pojawiające się zagrożenia dla tego typu systemów, i tym samym zagrożenia dla krytycznych usług w energetyce, gazownictwie, transporcie, medycynie itp. Punktem wyjścia do stworzenia systemu jest to, że użytkownicy SCADA mają specyficzne wymagania dotyczące funkcjonalności. Unikają aktualizacji tych systemów i nie poddają ich audytowi, stawiając tylko na działania reakcyjne, które niestety mogą się okazać spóźnione. Obecne systemy SCADA funkcjonują w zdecydowanej większości na bazie systemów Linux i Windows. Kaspersky pokusił się o próbę napisania zupełnie nowego systemu, który ma osiągnąć bezpieczeństwo dzięki bardzo drobiazgowemu i bezpiecznemu projektowi kodu już od poziomu jądra systemu. Nowy system ma być odporny na ataki takiego typu jak Stuxnet, Duqu czy Flame. Więcej informacji nie jest ujawnione ze względu na bezpieczeństwo samego systemu, jak i zapewnienie sobie przewagi konkurencyjnej. Więcej: http://bit.ly/Pz6lQL

li działania rozpoznawcze, nakierowane na zidentyfikowanie krytycznych systemów. Po tej identyfikacji przystąpili do ataku zasadniczego. Korzystając ze znanych hakerskich technik (tj.: ARP spoofing[1], phishing[2] czy atak DDoS[3]) doprowadzili oni ostatecznie do przejęcia praw administracyjnych w krytycznych systemach. Należy wyraźnie zaznaczyć, że atak odbywał się w środowisku, które nie odzwierciedlało rzeczywistego poziomu bezpieczeństwa „atakowanych" systemów. Te działania miały na celu przede wszystkim ilustrację zjawiska jakie mogłoby w rzeczywistości mieć miejsce i ukazać konsekwencję tego typu ataku. W tym przypadku konsekwencje były poważne – zakłócenie przekazu danych telemetrycznych i przejęcie kontroli nad urządzeniami kontrolującymi przepływ gazu, połączony ze wstrzymaniem tego przepływu na połączeniu międzynarodowym.

W tym samym czasie ćwiczenie przebiegało w warstwie organizacyjnej. Co to de facto oznaczało? Otóż oprócz kilkunastu osób zasiadających w centrum koordynacji ćwiczenia w centrum konferencyjnym Hali Stulecia, u dwóch najważniejszych „graczy" ćwiczenia – Gaz-Systemu i PSE Operatora, odbywały się realne działania proceduralne. Brało w nich udział kilkadziesiąt osób reprezentujących kilkanaście komórek organizacyjnych i stanowisk. Wymieniali oni pomiędzy sobą informacje, które odwzorowywały ich poczynania, zgodnie z przyjętymi procedurami reagowania na tego typu zdarzenia, jakie miały miejsce w środowisku laboratoryjnym. Takich przepływów informacji było około 600. Są one udokumentowane i mogą posłużyć do bardzo szczegółowej analizy poczynań poszczególnych graczy. Wszystko odbywało się na bazie przygotowanego scenariusza, który zawierał blisko 40 najróżniejszych zdarzeń (tzw. „injects"). Wiele z nich było zdarzeniami warunkowymi, które były uruchamiane tylko w sytuacji, gdy sami grający nie podjęli odpowiednich działań. Dzięki takim warunkowym zdarzeniom można było zrealizować w całości cele ćwiczenia. Przy okazji przypomnijmy je:

- Sprawdzić ZDOLNOŚĆ DO REAKCJI na atak oraz możliwości minimalizacji jego skutków
- Sprawdzić SKUTECZNOŚĆ INFORMOWANIA właściwych organów o ataku (identyfikacja właściwych organów, kanały łączności, jakość informacji)
- Sprawdzić ZDOLNOŚĆ DO WSPÓŁPRACY pomiędzy właściwymi organami administracji publicznej, "atakowanym" i innymi podmiotami.

Jak to sprawdzenie wypadło? Pełna odpowiedź na to pytanie nie jest jeszcze gotowa. Trwa analiza materiału ćwiczeniowego i wszystkie wnioski nie są jeszcze znane. Końcowy raport ujrzy światło dzienne 19 grudnia 2012 r. w trakcie konferencji zorganizowanej przy wsparciu Stowarzyszenia Euro-Atlantyckiego w Pałacu Lubomirskich w Warszawie. Niemniej jednak już teraz łatwo wskazać kilka istotnych spostrzeżeń.

Przede wszystkim zagrożenie atakiem, który w istotny sposób mógłby zakłócić działanie sieci dystrybucji gazu czy energii elektrycznej, jest jak najbardziej realne. Mimo, że jak wspomnieliśmy zabezpieczenia środowiska laboratoryjnego nie były rzeczywiste, to przy zaprezentowanej próbce zaawansowanych ataków jakie przeprowadził „red team" łatwo sobie wyobrazić, że to co stało się w laboratorium ćwiczenia Cyber-EXE Polska 2012, mogłoby stać się w real-

[1] http://pl.wikipedia.org/wiki/ARP_Spoofing
[2] http://pl.wikipedia.org/wiki/Phishing
[3] http://pl.wikipedia.org/wiki/DDoS

Uczestnicy IX konferencji „Wolność i Bezpieczeństwo" foto IDG

Uczestnicy Cyber – EXE 2012. Od lewej: Tadeusz Włodarczyk (PSE Operator SA), Grzegorz Kołaczek (Politechnika Wrocławska), Rafał Kasprzyk (Wojskowa Akademia Techniczna), Mirosław Maj (Fundacja Bezpieczna Cyberprzestrzeń), Kamil Kowalczuk (Gaz–System SA), Maciej Pyznar (Rządowe Centrum Bezpieczeństwa), Tomasz Zachmacz (Komenda Główna Policji), Krzysztof Tomkiel (Ministerstwo Obrony Narodowej), Michał Pawlak (Gaz-System SA), Marcin Brzeziński (Ministerstwo Obrony Narodowej), Aneta Trojanowska (Komenda Główna Policji), Artur Barankiewicz (TP Cert Orange), Artur Ślubowski (RWE Polska). Foto IDG.

nym środowisku. Skoro swego czasu skutecznemu atakowi, o gigantycznych konsekwencjach, uległa taka firma jak RSA Security[1] to dlaczego niby miałoby to nie zdarzyć się innym?

Innym wnioskiem, który śmiało można wskazać jest to, że organizacje biorące udział w ćwiczeniu bardzo dobrze radziły sobie z procedowaniem przypadków, które ogólnie w ich obszarze działania określane są jako te związane z zarządzaniem kryzysowym. To zresztą dość oczywiste. Jak słusznie zauważył jeden z przedstawicieli kadry zarządzającej PSE Operator mówiąc: „My cały czas działamy w trybie zarządzania kryzysowego". Niemniej jednak, w przypadku ćwiczenia Cyber-EXE Polska 2012 źródło sytuacji kryzysowej tkwiło w cyberprzestrzeni i ten fakt stanowił, że sytuacja była pewnego rodzaju nowością dla ćwiczących, czymś z czym nie mają jednak do czynienia na co dzień i co wprowadzało utrudnienie w działaniu i podejmowaniu decyzji. W szczególności tych, które miały na celu eliminację źródła zagrożenia.

Jeśli chodzi o działania skierowane na zewnątrz organizacji to wniosków również jest bardzo wiele. Są one co prawda ograniczone przez fakt, że nie wszystkie instytucje zdecydowały się na udział w ćwiczeniu i nie pozwoliło to na pełne sprawdzenie istniejących powiązań i wzajemnych relacji pomiędzy istotnymi podmiotami sektora publicznego i prywatnego. Nie oznacza to jednak, że to co zaobserwowaliśmy jest nieważne. Sygnalizując tylko pojawienie się pełnej listy wniosków, można przywołać chyba jeden z ciekawszych, a mianowicie ten, który mówi, że ćwiczący kontaktowali się ze „światem zewnętrznym" głównie w celach informacyjnych, wypełniając zapewne nałożony na nich obowiązek informacyjny. Wskazuje to na to, że chyba nadal jest wiele do zrobienia jeśli chodzi o nawiązywanie kontaktów, które służyć mają wspólnym działaniom zmierzającym do usunięcia problemu i minimalizacji jego skutków. Już powstają rekomendacje, które mają zmienić ten stan rzeczy. Za kilkanaście dni będzie można się z nimi zapoznać, a później będziemy zachęcali do tego, aby wdrożyć je w życie. Jest zresztą dokument, w którym można te rekomendacje wykorzystać - powstająca właśnie „Polityka Bezpieczeństwa Cyberprzestrzeni Rzeczpospolitej Polskiej". Zrobimy wszystko, aby praca wielu osób nie poszła na marne i aby kolejne edycje ćwiczenia Cyber-EXE 2012 udowadniały sens podjętego wysiłku.

Autor jest prezesem Fundacji Bezpieczna Cyberprzestrzeń. Z ramienia Fundacji koordynował przygotowanie i przebieg ćwiczenia Cyber-EXE Polska 2012.

CYBER-EXE POLSKA 2012

[1] http://blogs.rsa.com/anatomy-of-an-attack/

CYBER EUROPE 2012

Maciej Pyznar
Rządowe Centrum Bezpieczeństwa

Drugie ogólnoeuropejskie ćwiczenie w zakresie reagowania na zagrożenia z cyberprzestrzeni odbyło się w Grecji 4-5 października 2012 r. Miałem okazję reprezentować w nim Polskę jako obserwator.

Program dla obserwatorów skierowany był przede wszystkim do przedstawicieli krajów oraz organizacji, które nie uczestniczyły aktywnie w ćwiczeniu. Oprócz Polski w programie udział wzięli także przedstawiciele: Malty, Szwajcarii, Bułgarii, Wielkiej Brytanii, Komisji Europejskiej (DG CNECT, Wspólnego Centrum Badawczego – JRC, Sekretariatu Generalnego).

Status obserwatora w przeciwieństwie do aktywnych uczestników nie dawał pełnego wglądu w ćwiczenie, ale pozwolił mi w wystarczający sposób na śledzenie jego przebiegu.

Skąd w ogóle idea organizacji wspólnych, europejskich ćwiczeń?

30 marca 2009 r. Komisja Europejska wydała komunikat COM (2009) 149 "Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności". Wśród działań proponowanych we wspomnianym komunikacie są zmierzające do opracowania zasad i wytycznych dotyczących odporności Internetu oraz organizacji ogólnoeuropejskich ćwiczeń w zakresie reakcji na poważne incydenty naruszenia bezpieczeństwa sieci.

Podczas Konferencji Ministerialnej w Tallinie, która miała miejsce w kwietniu 2009 roku, ustalono plan działania w zakresie ochrony krytycznej infrastruktury teleinformatycznej. Podkreślono w nim, że "wspólne europejskie ćwiczenie w dziedzinie ochrony krytycznej infrastruktury teleinformatycznej powinno być zorganizowane i przeprowadzone w 2010 r., zgodnie z przyjętym przez Komisję planem działania...". Powyższe działania doprowadziły do organizacji ćwiczenia Cyber Europe 2010. Wsparcie ogólnounijnych ćwiczeń w zakresie zagrożeń z cyberprzestrzeni jest również jednym z głównych działań w ramach „Europejskiej agendy cyfrowej”[1].

W organizację ćwiczeń z cyklu Cyber Europe, zarówno w 2010 jak i 2012 roku, w roli koordynatora, zaangażowana była ENISA. Agencja już w 2009 r. wydała dokument metodyczny na temat organizacji ćwiczeń[2], co, wraz z przygotowaniem merytorycznym jej pracowników, ułatwiało podjęcia się tej roli.

Ale przejdźmy do samego ćwiczenia Cyber Europe 2012. Jego celem było:

1.Test efektywności i skalowalności istniejących mechanizmów, procedur i przepływu informacji w ramach współpracy władz publicznych w Europie;

2.Zbadanie współpracy podmiotów publicznych i prywatnych w przypadku poważnego ataku z cyberprzestrzeni w Europie;

3.Zidentyfikowanie luk i wyzwań w reakcji na poważne ataki z cyberprzestrzeni w Europie.

Jednym z wniosków z ćwiczenia Cyber Europe 2010[3] był brak procedur wymiany informacji o ataku z cyberprzestrzeni pomiędzy uczestniczącymi krajami. Konsekwencją braku wymiany informacji był również brak koordynacji działań pomiędzy zaatakowanymi, co potencjalnie prowadziło do nasilenia skutków ataku. Dlatego też jedną z najważniejszych rekomendacji była potrzeba stworzenia standardowej procedury operacyjnej (SOP z ang. *Standard Operational Procedure*) w zakresie wymiany informacji pomiędzy organizacjami z różnych krajów dotkniętych atakiem. Taka procedura powstała. Opiera się ona głównie na współpracy zaangażowanych podmiotów i w ćwiczeniu Cyber Europe 2012 miała zostać przetestowana.

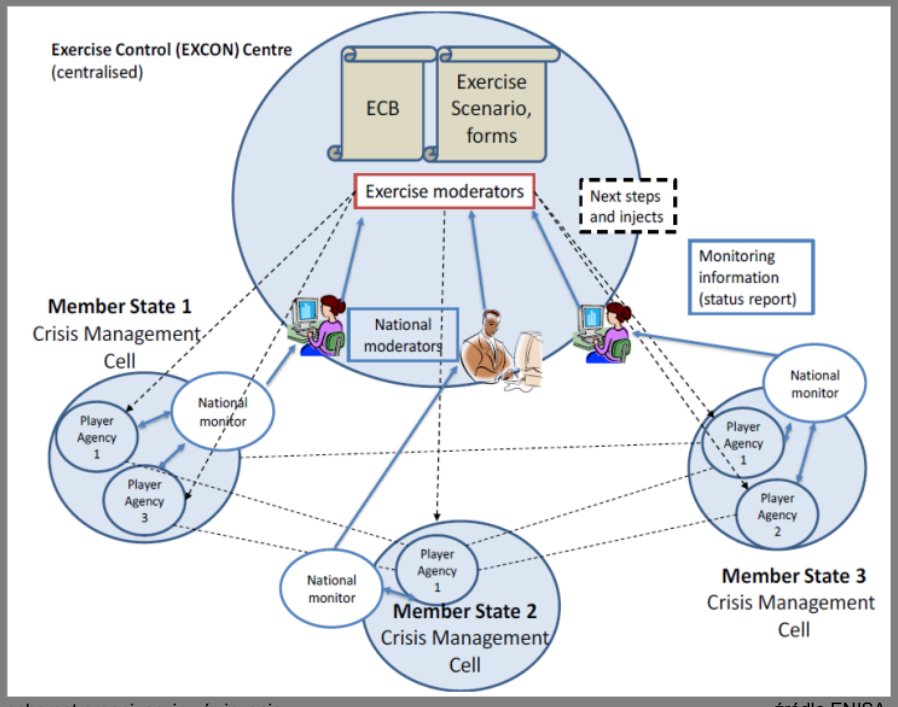
Samo ćwiczenie zostało poprzedzone ponad rocznymi przygotowaniami, w trakcie których zorganizowano kilkanaście warsztatów i spotkań. Głównym celem warsztatów było opracowanie scenariusza ćwiczenia, który w mojej ocenie był najsilniejszą stroną Cyber Europe 2012, ale o tym za chwilę.

W aktywnej fazie ćwiczenia uczestniczy-

[1] Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Europejska agenda cyfrowa – COM(2010)245 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PL:PDF

[2] „Good Practice Guide on National Exercises – Enhencing the Resillience of Public Communications Networks” - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises/national-exercise-good-practice-guide

[3] „Cyber Europe 2010 – Evaluation Report” - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report



schemat organizacyjny ćwiczenia źródło ENISA

ło 25 krajów, w tym 23 kraje członkowskie UE. Kraje były reprezentowane przez 339 organizacji, w tym m.in.: krajowe zespoły CERT (także CERT-y rządowe), podmioty z sektora finansowego (których dotyczył scenariusz), dostawcy Internetu, organy administracji publicznej.

Ogółem w ćwiczeniu zaangażowana była imponująca liczba ok. 600 osób.

Ćwiczenie Cyber Europe 2012 było rozproszonym ćwiczeniem sztabowym (z ang. *distributed table-top exercise*). Centrum Kontroli Ćwiczenia (CKC) znajdowało się w Markopoulo niedaleko Aten w miejscowym biurze ENISA. W CKC byli obecni także moderatorzy ćwiczenia oraz moderatorzy krajowi i obserwatorzy.

Ćwiczący przebywali w swoich miejscach pracy. Znajdowały się tam również osoby monitorujące ćwiczenie na poziomie krajowym. Byli oni "oczami i uszami" krajowych moderatorów. Ich zadaniem była obserwacja działań podejmowanych przez ćwiczących i przekazywanie raportów sytuacyjnych do moderatorów krajowych.

Podczas ćwiczenia aktywni uczestnicy mogli swobodnie komunikować się ze sobą, jak podczas normalnej działalności. W przypadku użycia poczty e-mail informacja musiała być wysłana do wiadomości osoby monitorującej. W celu kontroli przebiegu ćwiczenia moderatorzy otrzymywali raporty sytuacyjne wypełniane przez moderatorów krajowych i osoby monitorujące.

Ćwiczenie było wspierane przez portal ćwiczeń oparty na narzędziu EXITO (*the EXercise event Injection TOolkit*), opracowanym przez Instytut Ochrony Ludności JRC[1]. Wszyscy uczestnicy ćwiczenia mieli dostęp do portalu. Funkcjonalności oferowane przez portal zależały od roli uczestnika. Za pomocą portalu dystrybuowane były wprowadzenia do scenariusza oraz przekazywane raporty sytuacyjne. Na potrzeby CE2012 EXITO zostało rozbudowane o moduł pozwalający na zobrazowanie rozwoju sytuacji.

Przejdźmy jednak do najciekawszej sprawy – scenariusza. Przewidywał on wystąpienie ataków z cyberprzestrzeni na skalę ogólnoeuropejską, które dotknęły wszystkie kraje aktywnie uczestniczące. Scenariusz Cyber Europe 2012 łączył w sobie kilka technicznie realnych zagrożeń w jeden jednocześnie rosnący atak typu DDoS (z ang. *Distributed Denial of Service*) na publiczne i prywatne usługi elektroniczne. W efekcie miało to spowodować zakłócenia dla milionów obywateli w całej Europie.

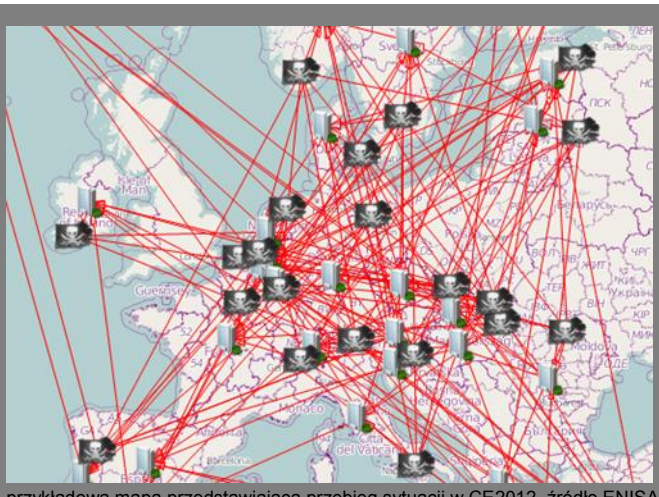
Atak przeprowadzili fikcyjni haktywiści, którzy połączyli siły w Cyber Punk Alliance (CPA). Motywacją CPA był sprzeciw wobec „zniewolenia ludzi przez rządy i posłuszne im instytucje finansowe". Wykorzystując podatność typu 0-day, czyli nieznane powszechnie, w tym nieznane producentom systemów i oprogramowania, przejęli oni kontrolę nad oprogramowaniem i powiązanymi bazami danych panelu Blesk. W ćwiczeniu jest to wspólna platforma do świadczenia usług administracyjnych drogą internetową (np. deklaracje podatkowe, rejestracja pojazdów itp.), którą można by określić usługą e-administracji. Blesk posłużył następnie do budowy botnetu – każdy logujący się do panelu ściągał nieświadomie na swój komputer złośliwe oprogramowanie. Nowością był sposób zarządzania botnetem. Otóż nie było jednego serwera CnC (z ang. *Command and Control*), ale w każdym z krajów ćwiczących znajdowały się po cztery, każdy z własnym URL. Do przeprowadzenia kolejnych faz ataku używano za każdym razem tylko 15 z tych serwerów. Zmiana serwerów następowała zgodnie z algorytmem czasowym. CPA za pomocą tak skonstruowanego botnetu mieli zaatakować rządowe usługi świadczone drogą elektroniczną oraz sektor finansowy.

Poloneza czas zacząć! O godz. 9:00 czwartego października Dyrektor Zarządzający ENISA prof. Udo Helmbrecht, przebywający w Estonii, w siedzibie estońskiego rządowego zespołu CERT (skąd miał obserwować przebieg ćwiczenia), połączył się telekonferencją z CKC i oficjalnie rozpoczął ćwiczenie Cyber Europe 2012.

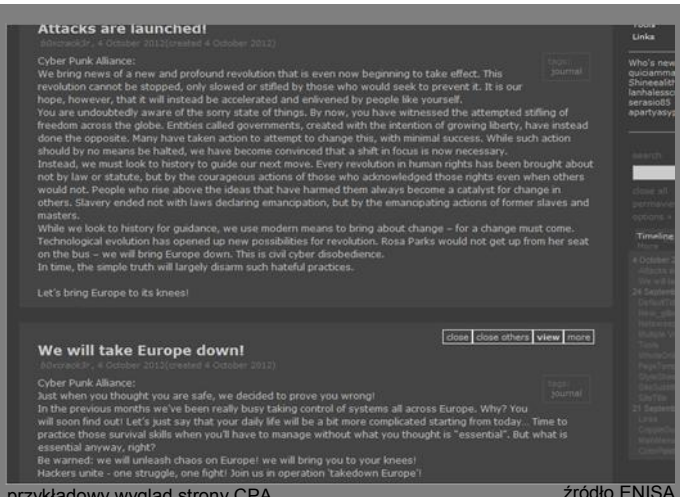
W tej chwili poprzez EXITO zostały wysłane pierwsze wprowadzenia. Zgodnie ze scenariuszem CPA skutecznie zaatakowali rządowe usługi świadczone drogą elektroniczną oraz sektor finansowy. Dostęp do usług ulegał degradacji, tak że około godziny 14:00 dostęp do wszystkich usług został zablokowany.

Aby podnieść realizm ćwiczenia zostały przygotowane również fikcyjne strony internetowe, które umożliwiały ilustrację rozwoju wydarzeń. Pierwszą była strona „atakujących". Na niej CPA publikowali manifesty, ale także informacje o nowych kierunkach i skuteczności ataku (które potwierdzane były następnie odpowiednimi wprowadzeniami ze scenariusza). Drugą była strona serwisu informacyjnego BCC (zbieżność nazwy z BBC oczywiście nie jest przypadkowa). Tu prezentowane były głównie informacje o skutkach ataku i reakcji sektora finansowego i rządów. Trzecią była strona blogera, ukrywającego się pod wiele mówiącym pseudonimem „Wszystkowiedzący Ryszard" (ang. *Richard I. Knowitall*), który starał się „rozgryźć" atakujących. Na tej stronie prezentowane były techniczne informacje o ataku i, co najważniejsze dla ćwiczących, wskazówki do rozwiązania problemu.

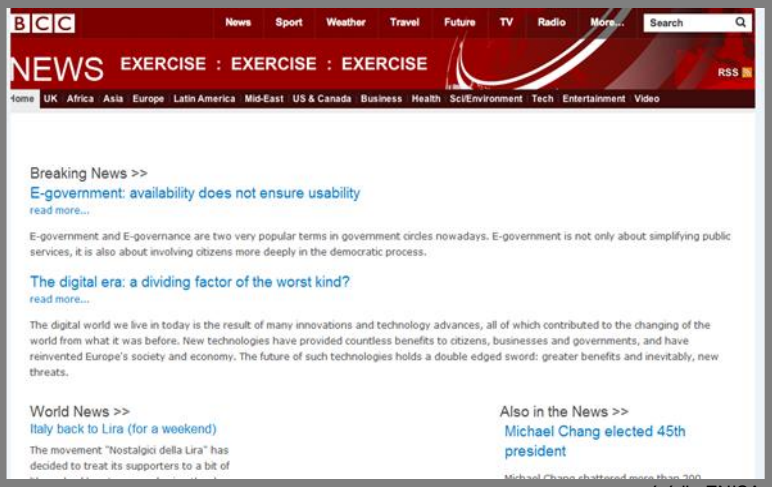
[1] EXITO jest darmowym, licencjonowanym oprogramowaniem open-source. Więcej informacji na temat EXITO - http://sta.jrc.ec.europa.eu/index.php/cip-home/75-exito/314-exito



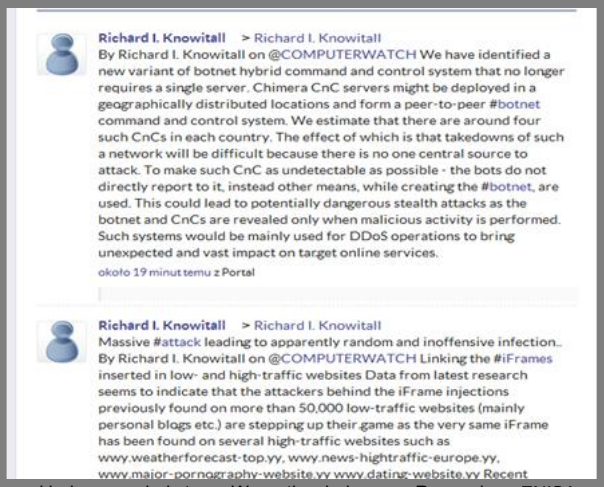
przykładowa mapa przedstawiająca przebieg sytuacji w CE2012, źródło ENISA



przykładowy wygląd strony CPA źródło ENISA



przykładowy wygląd strony BCC źródło ENISA



przykładowy wygląd strony Wszystkowiedzącego Ryszarda, ENISA

Ćwiczenie odbyły się na dwóch poziomach[1]: technicznym i operacyjnym. Na poziomie technicznym zadanie ćwiczących polegało na znalezieniu pełnej listy serwerów CnC oraz na znalezieniu algorytmu czasowego ataku (to zadanie najszybciej wykonał rządowy zespół CERT ze Szwajcarii). Na poziomie operacyjnym wykorzystana miała zostać SOP, co miało na celu wyzwolenie współpracy międzynarodowej i poprzez tę współpracę wykonanie zadań na poziomie technicznym oraz koordynację działań obronnych.

SOP przewiduje, że w sytuacji ataku z cyberprzestrzeni na większą liczbę państw, zawiązana zostanie grupa, która ma wspólnie reagować na zaistniałą sytuację. Na czele grupy ma stać koordynator (w oryginale *crisis facilitator*, co można by przetłumaczyć jako wspomagający rozwiązanie kryzysu). Koordynatorem może zostać kraj, którego najbardziej dotknął atak, który ma najlepsze techniczne możliwości do pełnienia tej roli lub kraj zaatakowany jako pierwszy. Ostateczna decyzja o tym, kto będzie pełnił tę rolę, jest podejmowana w drodze konsultacji między państwami (w ćwiczeniu została wykorzystana do tego celu telekonferencja). Ciekawostką z CE2012 było to, że w początkowej fazie ataku zawiązały się dwie grupy reagowania. W dalszej części ćwiczenia, po całkowitym zablokowaniu dostępu do usług, koordynatorzy uzgodnili, że rolę tę będzie pełnił jeden z nich (obserwatorzy nie mieli informacji o tym, których konkretnie organizacji z danego kraju dotyczyły uzgodnienia). Po tej fazie rozpoczął się stopniowo proces opanowywania kryzysu. Między innymi sukcesywnie odcinano komunikację z odnalezionych serwerów zarządzających atakami oraz odkryty został algorytm czasowy sterujący przełączaniem serwerów.

Około godziny 17:00 ćwiczenie zostało zakończone. W dniu następnym przeprowadzono na gorąco próbę podsumowania ćwiczenia oraz wstępnej jego oceny. Wstępne analizy i dyskusja pozwoliły na wyciągnięcie następujących wniosków:

1.Zaobserwowano różne podejścia do rozwiązania problemu ataku. Były kraje, które eskalowały sprawę do poziomu politycznego (odpowiadającego polskiemu Rządowemu Zespołowi Zarządzania Kryzysowego), były również takie, które pozostawiły rozwiązanie na poziomie stricte technicznym.

2.SOP się sprawdziła i okazała się bardzo przydatna, choć wystąpiły problemy koordynacyjne.

3.Przygotowana lista kontaktowa okazała się niekompletna i istnieje konieczność jej uzupełnienia.

4.Wystąpiły różnice w formacie przekazywanych poprzez raporty sytuacyjne informacji. W związku z tym istnieje konieczność uzupełnienia SOP o standaryzowany format raportów cząstkowych do stworzenia wspólnego raportu sytuacyjnego.

Z mojego punktu widzenia było to niezwykle ciekawe doświadczenie. Zaledwie dwa tygodnie wcześniej przeprowadzone zostało w Polsce ćwiczenie CYBER-EXE POLSKA 2012 (o którym możecie Państwo przeczytać również w bieżącym numerze „CIIP focus", w artykule Mirosława Maja), w którym również uczestniczyłem. Zainteresowany byłem zatem stroną organizacyjną. Szybka analiza porównawcza doprowadziła mnie do konstatacji, że w obliczu zagrożeń z cyberprzestrzeni wszyscy dzielimy podobne doświadczenia i prawdopodobnie możemy zastosować podobne rozwiązania. Pozostaje mieć nadzieję, że w następnych ćwiczeniach z cyklu CYBER EUROPE Polska będzie odgrywać rolę aktywnego uczestnika. Czego sobie i Państwu życzę.

Autor jest głównym specjalistą w Wydziale Ochrony Infrastruktury Krytycznej Rządowego Centrum Bezpieczeństwa, absolwentem Wydziału Nawigacji i Uzbrojenia Okrętowego Akademii Marynarki Wojennej oraz Studium Bezpieczeństwa Narodowego Uniwersytetu Warszawskiego. W RCB, w którym pracuje od momentu utworzenia tej instytucji, zajmuje się działaniami planistycznymi i programowymi w zakresie ochrony infrastruktury krytycznej.

[1] Decyzje podejmowane na poziomie politycznym nie były brane pod uwagę w scenariuszu. Obecnie toczy się dyskusja jak i kogo poziomu politycznego zaangażować oraz w jaki sposób w przyszłych ćwiczeniach na ten poziom eskalować zdarzenia w scenariuszu

ABUSE Forum
historia powstania i zakres działania

Mirosław Maj

Ponad siedem lat temu, w Warszawie odbyło się pierwsze spotkanie przedstawicieli polskich zespołów reagujących na przypadki naruszenia bezpieczeństwa w sieci. Spotkanie odbyło się z inicjatywy i w siedzibie NASK, a dokładniej rzecz biorąc, działającego w jej ramach zespołu CERT Polska.

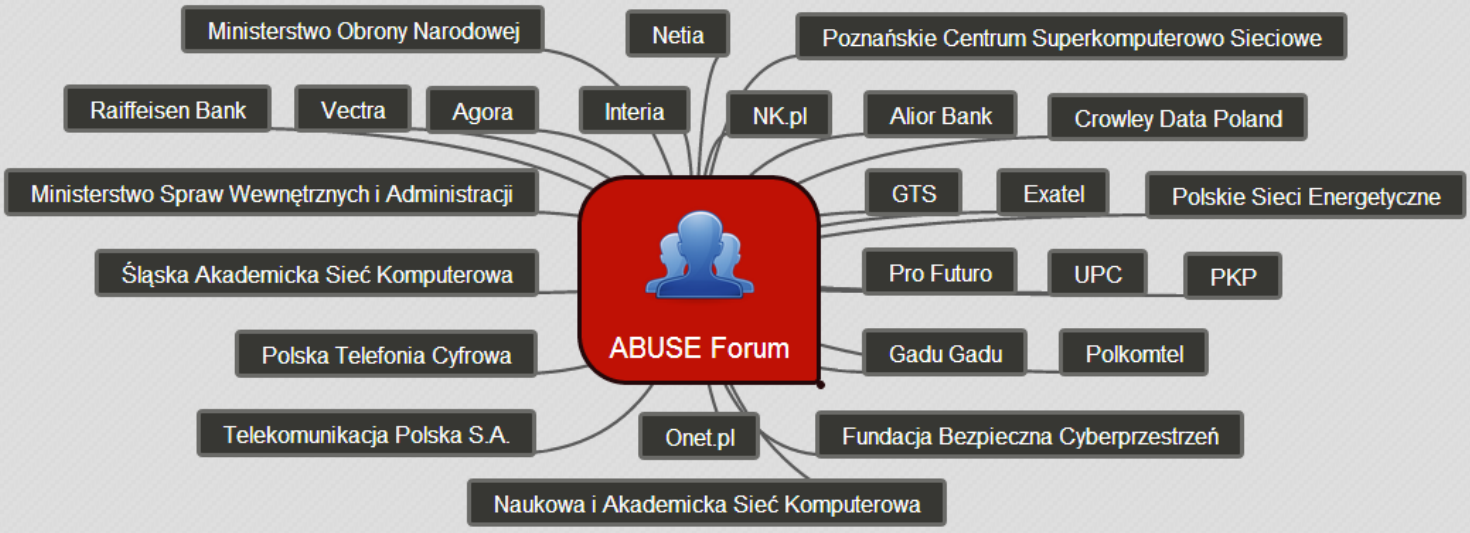
Kierując w tamtym czasie zespołem CERT, miałem przyjemność otworzyć to spotkanie i przybliżyć uczestnikom ideę powołania do życia stałego forum wymiany doświadczeń i informacji. To zadanie się udało, gdyż forum, któremu później nadano nazwę Abuse Forum, zaczęło działać systematycznie i do dziś odbyło się już dwadzieścia spotkań, które organizowane są mniej więcej co cztery miesiące. Najczęściej spotkania odbywają się w Warszawie, w siedzibie NASK, ale w długiej historii działania członkowie Forum mieli również okazję korzystać z gościnności Poznańskiego Centrum Superkomputerowo-Sieciowego, Ministerstwa Obrony Narodowej, Politechniki Śląskiej w Gliwicach czy T-Mobile SA.

Rozpoczynając w 2007 r. tę inicjatywę chcieliśmy przenieść na polski grunt nasze szerokie doświadczenia międzynarodowe. W innych krajach, w tamtym czasie, fora wymiany doświadczeń już funkcjonowały. Było tak np. w Niemczech czy Holandii. Dodatkowo, modele współpracy międzynarodowej, takie jak FIRST[1] czy TERENA TF-CSIRT[2], również doskonale nadawały się do zastosowania, oczywiście przy zachowaniu odpowiedniej skali przedsięwzięcia.

Na pierwsze spotkanie Abuse Forum, przed siedmioma laty, przybyli przedstawiciele 11 organizacji: ASTER, Exatel, Poznańskie Centrum Superkomputerowo-Sieciowe (Pionier-CERT), PKP Informatyka, Polkomtel, PSE, Telekomunikacja Polska, Telekomunikacja Kolejowa, UPC, VECTRA i NASK (CERT Polska). Większość z nich do dnia dzisiejszego jest członkami Forum. Po drodze niektórzy „odpadli", ale też pojawiło się kilka nowych organizacji. Do grupy dołączyli przedstawiciele „istotnych graczy" w „polskim Internecie", takich jak Onet, Interia, Gadu-Gadu, Allegro czy NK.pl. W pewnym momencie podjęto decyzję o dołączeniu do grona współpracujących zespołów, komórek, które tworzyły się w ramach struktur administracji państwowej, a mianowicie zespołu rządowego CERT.GOV.PL oraz wojskowego zespołu CERT-owego noszącego nazwę „Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych MON". Jeszcze później grono powiększyło się o sektor finansowy w postaci przedstawicieli banków - Raiffeisen Bank i Alior Bank. Swoją drogą przedstawiciele drugiego z nich stworzyli pierwszy w Polsce zespół typu CERT działający w sektorze finansowym[3]. Wreszcie w 2010 roku do Forum dołączyła organizacja typu NGO, a mianowicie Fundacja Bezpieczna Cyberprzestrzeń. Dzisiaj Abuse Forum liczy 25 członków o najróżniejszym profilu działalności[4].

Pierwotnym zamysłem było połączenie sił i doświadczeń głównie operatorów telekomunikacyjnych. Można powiedzieć, że założenie to się nie sprawdziło, choć trudno byłoby to uznać za porażkę. Każda z organizacji, właśnie przez fakt różnorodności formuły działania, jest w stanie wnieść w tę współpracę inną, cenną wartość.

[1] Forum of Incident Response and Security Teams – http://www.first.org/
[2] Trans European Research and Academic Networks Association Task Force for Computer Security Incident Response Teams
[3] Więcej o tym można przeczytać w wywiadzie z liderem tego zespołu – Przemysławem Skowronem: http://goo.gl/XgRZZ
[4] patrz: http://www.abuse-forum.pl/



za: www.abuse-forum.pl

Pierwszy okres działalności Forum to w dużej mierze poruszanie dwóch ważnych tematów. Po pierwsze, jak w praktyce działają poszczególne zespoły wewnątrz swoich organizacyjnych struktur, po drugie, jakie są doświadczenia ze współpracy z podmiotami zewnętrznymi, a w szczególności z organami ścigania. Te doświadczenia były niezwykle przydatne w praktyce. Przedstawiciele poszczególnych organizacji opowiadali o tym, jak radzą sobie w swoich sieciach ze spamem, z niesfornymi klientami, obsługą masowych zgłoszeń (np.: związanych z naruszeniem praw autorskich) itp. Mówili też o tym, z czym sobie nie radzą i wtedy zawsze można było liczyć na pomoc i podpowiedź innych, którzy podobny problem mieli już za sobą, albo po prostu wpadli na dobry pomysł jak dany problem rozwiązać. Niejednokrotnie na spotkaniach pojawiali się zaproszeni goście z Komendy Głównej Policji i godzinami omawialiśmy z nimi najlepsze praktyki w wymianie informacji w obydwu kierunkach, tak aby wzajemnie ułatwić sobie pracę.

W późniejszej działalności Forum pojawiły się również inne zagadnienia, takie jak zwalczanie nielegalnych treści w Internecie, wymiana informacji technicznej na temat zagrożeń w „polskim" Internecie, udostępnianie informacji organom ścigania w oparciu o platformę techniczną, działania złośliwego oprogramowania czy radzenie sobie z problemem „czarnych list" prowadzonych przez niektóre ośrodki bezpieczeństwa (np.: Spamhause). Na spotkaniach pojawiała się również dość często tematyka legislacyjna, w szczególności kiedy niektóre z osób pojawiających się na spotkaniach również aktywnie uczestniczyli w procesach legislacyjnych dotyczących bezpieczeństwa informacji, jakie miały i mają miejsce w Polsce.

Forum ma na swoim koncie również poważny sukces jeśli chodzi o wspólny projekt techniczny. Kilka lat temu udało się uruchomić wspólną platformę usługi „blackholing", dzięki czemu operatorzy telekomunikacyjni, którzy do niej dołączyli, dostali dostęp do narzędzia, którego mogą używać w zwalczaniu wielu zagrożeń w swojej sieci, a w szczególności ataków typu Distributed Denial of Service.

Abuse Forum jest pewnego rodzaju tworem nieformalnym. Wielokrotnie członkowie Forum omawiali kwestię tego czy właśnie ma tak być, czy bardziej odpowiednia mogłaby być formuła stowarzyszenia. Obydwa rozwiązania mają oczywiście swoje wady i zalety. Podstawową zaletą obecnie przyjętej formuły nieformalnych spotkań jest możliwość efektywnego i elastycznego działania operacyjnego w tych wszystkich przypadkach, kiedy przepisy prawne na to pozwalają. Pewną wadą jest natomiast to, że Forum ma utrudniony kontakt ze „światem zewnętrznym". Zabranie wspólnego głosu w ważkiej sprawie jest trudne, gdyż wymaga akceptacji i akredytacji praktycznie wszystkich członków, a tak naprawdę osób zarządzających w organizacjach. Ten kto próbował uzgodnić wspólne zdanie, więcej niż chociażby trzech instytucji, wie na czym polega problem. Rezultat – przez wiele lat działalności Abuse Forum praktycznie tylko raz przekazano na zewnątrz wspólne stanowisko. W lutym 2010 r. zgodnie ustalono, że „przeglądarka Internet Explorer w wersji 6.x jest niebezpieczną aplikacją". Taki komunikat pojawił się na stronach informacyjnych kilku członków Forum. Wtedy koordynowałem proces wspólnych uzgodnień, i proszę mi uwierzyć, nie było to zadanie łatwe. Mając na uwadze tamte doświadczenie nie zaryzykowałbym stwierdzenia, że wspólne stanowisko w poważniejszej sprawie jest w ogóle możliwe do wypracowania przez Abuse Forum. Nie znaczy to jednak, iż zmiana formuły jest konieczna.

Kiedy w 2009 i 2010 roku toczyły się pierwsze prace nad tym, co dzisiaj jest prezentowane jako projekt „Polityki Bezpieczeństwa Cyberprzestrzeni Rzeczpospolitej Polskiej"[1] pojawiła się szansa na to, że Abuse Forum zostanie wyraźnie wskazane w tej Polityce jako istotny element w rozwoju współpracy pomiędzy zespołami reagującymi w Polsce. Niestety, mimo gotowych koncepcji takiego rozwoju Forum i jego roli w całości systemu bezpieczeństwa cyberprzestrzeni RP, tak się nie stało. W dzisiejszej wersji dokumentu praktycznie o tej możliwości się nie wspomina. Jedynie można się domyślać z niektórych zapisów, że Forum może być sposobem wymiany informacji pomiędzy sektorem publicznym i prywatnym. To już jednak inny problem, który miejmy nadzieje znajdzie swój pozytywny finał.

Po wielu latach działalności Abuse Forum można wskazać jego wady i zalety. Jak każda inicjatywa, tak i Abuse Forum potrzebuje działań usprawniających, co pozwoliłoby na osiągnięcie kolejnego poziomu wartościowej współpracy i skutecznego sprostania ważnym i trudnym wyzwaniom. Niezależnie od tego, co najmniej jednej uniwersalnej wartości nie sposób przecenić. A mianowicie nawiązano dziesiątki kontaktów personalnych, które sprawiły, że współpraca operacyjna pomiędzy osobami bezpośrednio odpowiedzialnymi za bezpieczeństwo bardzo ważnych elementów „polskiego" Internetu stała się efektywna. Osobista znajomość ekspertów, z którymi trzeba na co dzień rozwiązywać problemy jest bardzo cenna. Najlepiej zresztą to opisuje misja tej inicjatywy:

Abuse Forum Polska to nieformalna organizacja zrzeszająca przedstawicieli największych polskich operatorów telekomunikacyjnych, dostawców Internetu, portali społecznościowych, a także organów administracji publicznej, w tym ministerstw i urzędów centralnych. Kwartalne spotkania oraz lista dyskusyjna służą poprawie komunikacji i zacieśnieniu znajomości, dzięki czemu możemy być jeszcze skuteczniejsi w prewencji i reagowaniu na pojawiające się w sieci zagrożenia.

Niejednokrotnie mieliśmy tego potwierdzenie w ostatnich siedmiu latach i miejmy nadzieję, że nie gorzej będzie w następnych.

Autor jako były kierownik zespołu CERT Polska (NASK) brał udział w powstaniu inicjatywy Abuse Forum.

[1] http://mac.bip.gov.pl/prawo-i-prace-legislacyjne/polityka-ochrony-cyberprzestrzeni-rp-resortowe-zglaszanie-uwag-do12-10-2012.html

Bezpieczeństwo

SCADA

to nie „Rocket Science”

Kamil Kowalczuk
Gaz-System SA

Uwarunkowania historyczne, czyli jak to było robione kiedyś

Kilkanaście lat temu miałem okazję zetknąć się z pojęciem SCADA (Supervisory Control And Data Acquisition). Systemy sterowania, telemetria, automatyka - pojęcia na tamte czasy dość abstrakcyjne dla informatyka. Wtedy nikt nie nazywał systemów sterowania istotnym elementem infrastruktury krytycznej, ale zapewne był on postrzegany jako ważny element infrastruktury, którego funkcjonowanie było kluczowe do zapewnienia ochrony i bezpieczeństwa energetycznego kraju. Informatycy uczyli się jak utrzymać dany system, a biznes – jak obsługiwać i z niego korzystać. Niemal idealny podział ról… Zaraz, a gdzie w tym wszystkim bezpieczeństwo?

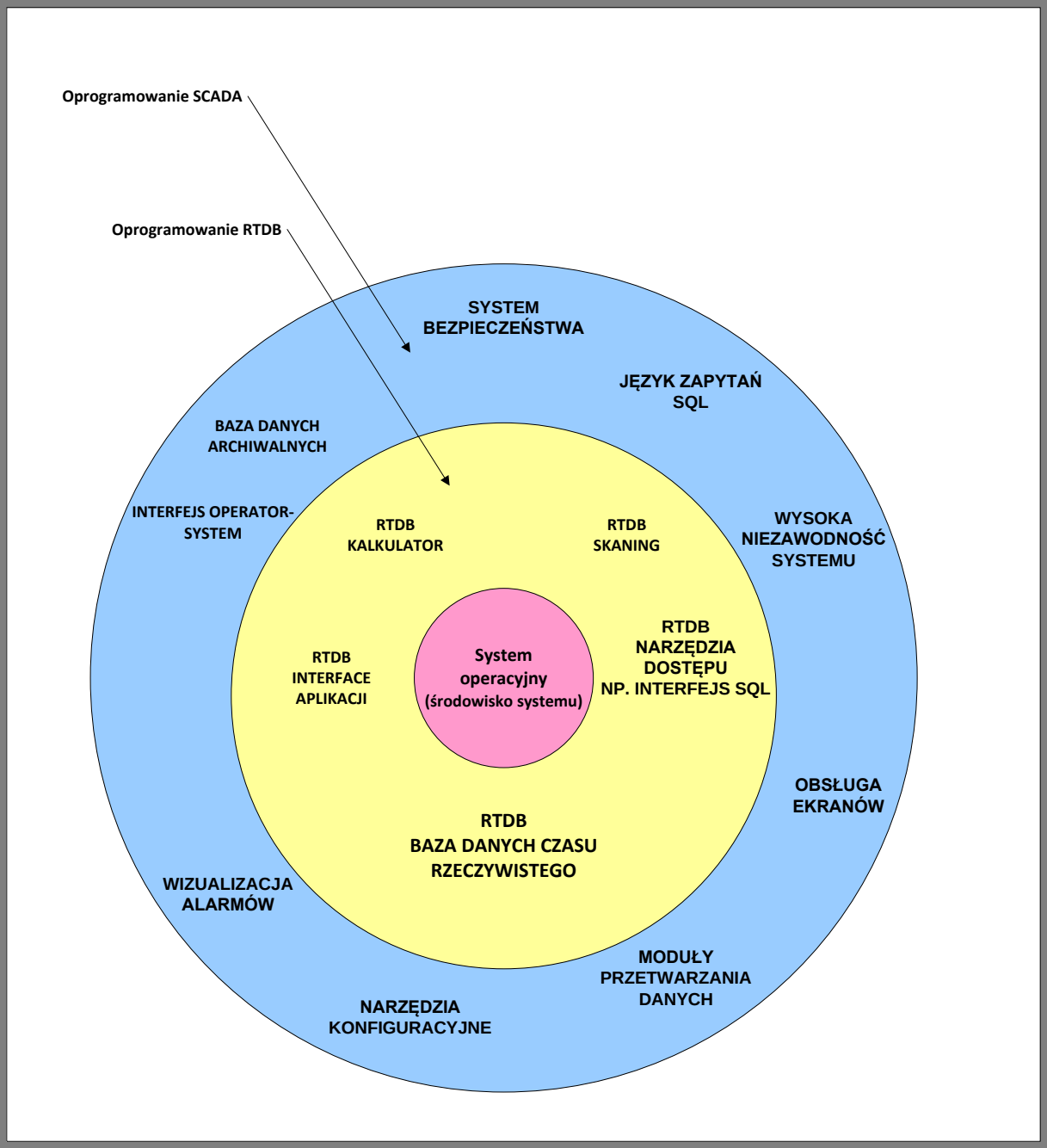
Należy zauważyć, że systemy SCADA użytkowane dotychczas zostały wdrożone w realiach ubiegłego wieku. Były zamknięte, odseparowane od świata zewnętrznego czyli teoretycznie, bezpieczne. Można więc było powiedzieć, że cyberzagrożenia nie występowały w systemach SCADA. Nie rozwijano zagadnienia bezpieczeństwa sygnału przesyłanego do sterownika koncentrując się na zapewnieniu ciągłości pracy systemu. Świat „informatyki przemysłowej” rządzi się odmiennymi prawami, często separując się od „informatyki ogólnej”, przynajmniej tak brzmiała ówczesna teoria o bezpieczeństwie systemów klasy SCADA. Rozwój technologiczny w szczególności w teleinformatyce i wzajemne przenikanie się systemów IT nie pozwolił na przetrwanie tego sztucznego podziału. Świadomość krytyczności systemów sterowania obecnie została dostrzeżona i coraz częściej jest poruszana przy okazji dyskusji o bezpieczeństwie teleinformatycznym.

Systemy SCADA są obecnie szeroko stosowane. Bez nich nie jest możliwe skuteczne prowadzenie ruchu, a co za tym idzie zapewnienie dostaw np. energii elektrycznej, ropy, gazu czy wody. Teleinformatyka jako dział zajmujący się transmisją informacji stał się niezbędnym elementem systemów nadzoru oraz sterowania. Powrót do sterowania „ręcznego” wymagałby przeorganizowania pracy całych przedsiębiorstw, co nie odbyłoby się bez uszczerbku dla ciągłości dostaw.

Czym właściwie jest system sterowania i nadzoru (SCADA)?

Spróbujmy spojrzeć na system nie jak na „czarną skrzynkę”, ale jak na każdy inny system teleinformatyczny funkcjonujący w organizacji. SCADA zbiera dane, odpowiednio prezentuje oraz na podstawie uzyskanych informacji odpowiednio steruje procesami technologicznymi. Elementem łączącym poszczególne funkcjonalności, niekiedy moduły, jest sieć poprzez którą komunikuje się cały system. Aktualnie, na potrzeby środowiska wykorzystuje się z powodzeniem komunikację IP, często „opakowując” starsze protokoły wykorzystywane pierwotnie w połączeniach szeregowych na stacjach pomiarowych (RTU). Protokoły technologiczne wykorzystuje się w bezpośrednim połączeniu ze sterownikiem (PLC). W systemie SCADA występuje również szereg aplikacji wspomagających (np. prognozujących, czy symulujących przepływ w sieciach gazowych lub wodno-kanalizacyjnych) – są to stałe elementy systemu.

Kolejną typową i powszechnie znaną cechą tego systemu są interfejsy umożliwiające import/eksport danych pomiarowych w celu wymiany pomiędzy innymi systemami SCADA oraz niekiedy z systemami rozliczeniowymi (dane dzieli się często na „ruchowe” - niezbędne do prawidłowego sterowania i „rozliczeniowe” – niezbędne do rozliczeń finansowych). Kto z nas nie płaci rachunków za energię elektryczną, wodę czy gaz? Wszystkie te elementy budują nam system, który ma na celu pomóc służbom dyspozytorskim w skutecznym nadzorze i sterowaniu „elementami infrastruktury krytycznej”. Przechodząc na język biznesowy, wspomaga on kluczowy proces w organizacji - „core-biznes”.



przykładowa struktura programowa

Zbliżone moduły i funkcjonalność posiadają inne systemy teleinformatyczne wymagające przechowywania, przetwarzania i prezentacji danych informacyjnych. Czy systemy finansowo-księgowe, kadrowo-płacowe, bilingowe nie wymagają kolekcjonowania, przechowywania, przetwarzania i prezentacji danych informacyjnych? Czym one się różnią od systemów sterowania? Kolejnym pytaniem, jakie można sobie zadać – w jaki sposób systemy (np. bilingowe) kolekcjonują informacje? Co jest źródłem tych informacji i jak one trafiają do baz czy hurtowni danych?

W świetle znanych dobrych praktyk, udokumentowanych testów i sprawdzeń na tym etapie możemy dojść do istotnego wniosku - rozdzielenie fizyczne systemów sterowania od systemów informatyki ogólnej jest fikcją i w większości przypadków zawsze nią było. Systemy wspomagające procesy biznesowe wymagają dostępu do danych, również pobieranych bezpośrednio i na bieżąco z systemów klasy SCADA.

Architektura aplikacji stosowanych w systemach sterowania nie odbiega od ogólnie stosowanych przy projektowaniu systemów informatycznych. Różnica pojawia się w randze systemu. SCADA jest nie tylko kluczowa dla funkcjonowania przedsiębiorstwa, wspierając główne procesy biznesowe, ale również ingeruje bezpośrednio w prawidłowe i stabilne funkcjonowania Państwa, jako organizacji.

Jeśli już otrząsnęliśmy się i mentalnie nastawiliśmy na istotę bezpieczeństwa systemów SCADA, jak każdego innego istotnego dla organizacji systemu, to mamy ogromne szanse powodzenia. Przyjdą nam z pomocą prawidła, normy oraz standardy funkcjonujące od dawna w szeroko rozumianej informatyce ogólnej. Uświadomimy sobie, że zabłąkany router WIFI w sieci biurowej, czy wpięta druga karta sieciowa w serwerze lub stacje robocze SCADA mogą stać się groźną podatnością. Spotyka się tego typu rozwiązania, zainstalowane często kilka lat temu, jako rozwiązanie tymczasowe, prowizoryczne, a przecież „prowizorki" są najbardziej trwałe. W tym przypadku nie jest inaczej.

Jak podejść do zabezpieczenia systemu?

Zacznijmy od podstaw, od części analitycznej – najpierw musimy wiedzieć co, żeby móc powiedzieć jak. Przeprowadźmy gruntowną analizę ryzyka, zidentyfikujmy podatności systemu, tak jak robimy to dla innych systemów i środowisk kluczowych dla funkcjonowania głównych procesów w przedsiębiorstwie np. systemu autoryzacji i zarządzania użytkownikami, systemu klasy ERP czy sieci korporacyjnej. Zweryfikujmy, które podprocesy obsługiwane w systemie nadzoru i sterowania są niezbędne do prawidłowego spełnienia obowiązków stawianych organizacji, posiadającej obiekty zaklasyfikowane jako infrastruktura krytyczna Państwa. Gruntownie przeprowadzona analiza z pewnością wykaże wiele punktów wspólnych dla sieci korporacyjnej i technologicznej, dla systemów biznesowych i systemów sterowania oraz dla procedur utrzymaniowych i eksploatacyjnych obydwu środowisk.

Co wymaga ochrony w systemach sterowania i nadzoru?

Już sobie powiedzieliśmy, że systemy sterowania i nadzoru mają wiele wspólnego z innymi systemami biznesowymi, a można nawet zaryzykować stwierdzenie, iż praktycznie się od nich nie różnią. Co w takim razie jest w nich najistotniejsze? Informacja! To informacja powinna być szczególnie chroniona w oparciu o znane i stosowane w systemach IT standardy bezpieczeństwa (są one definiowane przez ekspertów z danego obszaru IT np. w „dobrych praktykach").

Spoglądając od strony sterowania – chronione powinny być dane telemetryczne przesyłane do sterowników (PLC) oraz dane przesyłane z punktów pomiarowych do systemu. Przeważnie nie jest ważna ich poufność, gdyż specyfika prowadzonego biznesu wpływa na bardzo krótki czas ważności danych (dane „ruchowe"), najważniejsze, aby dane były pewne i realne, zabezpieczone w określonym przedziale czasu. Przecież to na ich podstawie systemy SCADA wspomagają dyspozytora w podjęciu decyzji, jak odpowiednio kierować przepływem czy linią technologiczną. Kompromitacja któregokolwiek z przesyłanych parametrów może oznaczać zaburzenie bądź zatrzymanie głównych procesów biznesowych przedsiębiorstwa.

Medium transmisyjnym dla systemów SCADA jest sieć – ta sama, która pozwala na komunikację pomiędzy innymi systemami biznesowymi danej organizacji. Standardowo uruchamiamy w niej zabezpieczenia w postaci segmentacji, firewall, sond IPS/IDS czy innych, znanych i powszechnie stosowanych systemów bezpieczeństwa. Standardowo, ale często z wykluczeniem segmentu sieci obsługującej środowisko SCADA i tu tkwi największy błąd i zaniedbanie.

Rozwiązania bezpieczeństwa należy stosować globalnie i w równym stopniu zabezpieczać wszystkie punkty środowiska teleinformatycznego. Czy nie jest słuszna teoria ograniczeń Williama Jamesa, która mówi iż „łańcuch jest tak mocny, jak jego najsłabsze ogniwo"? Przy obecnym stopniu integracji środowisk informatycznych, sieć teleinformatyczną należy traktować jako całość i nie można wykluczyć sytuacji, w której wykorzystując podatności jednego środowiska np. SCADA, uzyskamy dostęp do środowiska innego – np. systemu klasy ERP.

Patrząc na problem z drugiej strony: atakowanie bezpośrednio systemu sterowania i nadzoru nie jest konieczne. Można zaatakować bazę danych, czy system operacyjny, w którym podatności są ogólnie znane. Skonstruowanie nowego zagrożenia (np. typu „Zero Day") na ogólnie używany i udokumentowany element systemu funkcjonującego „w ramach środowiska SCADA" jest prostsze. W dobie scentralizowania systemów zarządzania uprawnieniami, stosowania jednokrotnego uwierzytelniania, możliwym staje się dostęp do systemu sterowania poprzez np. skompromitowany kontroler domeny. Uzyskanie dostępu do stacji roboczych w organizacji otwiera nam drogę do danych telemetrycznych oraz możliwości sterowania elementami infrastruktury technicznej.

Wróćmy do pojęcia „pełnej separacji" i izolacji systemów. Przez tego typu podejście sami tworzymy podatności. Wyobraźmy sobie sytuację, w której system dostarczający dane jest niemalże galwanicznie odizolowany od systemu odpowiedzialnego za wystawianie faktur klientom. Aby dane zostały przetransferowane, wykorzystywana jest np. pamięć przenośna typu pendrive. Staje się ona zagrożeniem dla systemu, poprzez brak spójności systemu z otoczeniem w aspekcie zarządzania.

Jedną z historii przytaczanych przez specjalistów od bezpieczeństwa jest opowieść o pewnej instytucji finansowej, która zbudowała świetne zabezpieczenia sieciowe. Byli spokojni o funkcjonowanie swoich systemów. Osoby, które chciały skompromitować system rozrzuciły „pen drivy" w okolicy siedziby firmy. Umieszczenie pamięci w zwykłej stacji roboczej pozwoliło obejść zabezpieczenia i dostać się do środka organizacji. Takich przykładów można przytaczać więcej - odpowiednio spreparowana wiadomość elektroniczna, ciekawa strona internetowa. Nie zapominajmy zatem o podnoszeniu świadomości wśród pracowników. Odpowiednio ukierunkowane szkolenia, prezentacje oraz dbanie o przestrzeganie zasad organizacyjnych wielokrotnie może być skutecznym elementem ochrony zasobów informacyjnych, również wtedy, gdy stosowane zabezpieczenia techniczne są najwyższej klasy.

Należy w równym stopniu zadbać o bezpieczeństwo wszystkich systemów działających w obrębie sieci korporacyjnej. Zabezpieczenie powinno odbywać się w myśl zasady „tylko niezbędny dostęp dla podtrzymania procesów biznesowych". Zabezpieczamy w równym stopniu serwery finansowe oraz systemy SCADA. W zależności od przeprowadzonej analizy ryzyka zwiększamy, bądź zmniejszamy poziom zabezpieczeń. Już na etapie planowania należy wybierać takie systemy sterownia i nadzoru, których środowisko pracy (otoczenie), można skutecznie zabezpieczyć i monitorować.

Jest wiele sposobów, metod, dobrych praktyk, wykorzystywanych na co dzień do zabezpieczania środowisk teleinformatyki biznesowej, które możemy, a nawet powinniśmy wykorzystywać w równym stopniu w odniesieniu do systemów SCADA. Musimy pamiętać o cyklicznej aktualizacji systemów operacyjnych, analizie podatności i zabezpieczaniu baz danych czy stosowaniu systemów zarządzania zgodnych z obowiązującymi normami, nie wykluczając certyfikacji w zakresie bezpieczeństwa informacji.

Czasy hakerów samotnie siedzących w piwnicy minęły bezpowrotnie. Osoby przygotowujące ataki to często specjaliści w swojej dziedzinie. Nie lekceważmy ich, to często świetne zespoły pracujące wręcz projektowo. Tworzą oni programy wykorzystujące błędy w oprogramowaniu (exploity), czy robaki komputerowe (w przeciwieństwie do wirusa, program który nie wymaga nosiciela). Ostatnie,

analizy użytych tego typu programów przeciwko systemom sterowania wykazały, że stworzyły je najprawdopodobniej bardzo dobrze zorganizowane zespoły, które miały pełną świadomość architektury i metod działania systemów, które stały się celem ich ataku.

Klika praktycznych porad…

To, że zbudowaliśmy separację logiczną, strumień danych został przepuszczony przez kilka firewalli nie zwalnia nas z zastosowania zabezpieczenia w systemach czy aplikacjach. Zbierajmy zdarzenia bezpieczeństwa z sieci SCADA, ale również z kontrolerów domeny, serwerów poczty, czy urządzeń aktywnych (sieciowych) i korelujmy je razem. Twórzmy standardy konfiguracyjne i trzymajmy się ich, tak samo w środowisku aplikacji czy sieci.

Przeprowadzajmy weryfikację bezpieczeństwa systemów również po przez specjalistów zewnętrznych. Traktujmy audyt, jako narzędzie w samodoskonaleniu systemu, który mamy za zadanie chronić. Weryfikujmy aktualność dokumentacji technicznej systemu. Pomoże nam ona w przypadku rozwoju systemu i pozwoli uniknąć wielu błędów architektonicznych, które mogą tworzyć kolejne słabe punkty. Opierajmy się na standardach zarządzania, stosowanych od dawna w informatyce, między innymi ITIL, ISO/IEC 20000. Czytajmy przewodniki producentów, normy i standardy bezpieczeństwa np. NIST, ISO/IEC 27001. Przekazują one wiedzę niezależnie od stosowanej technologii, wyznaczając kierunek i definiują wzorce postępowania. Projektujmy systemy SCADA w sposób przemyślany, ale nie w oderwaniu od funkcjonujących systemów wspomagających procesy biznesowe.

Holistyczne podejście do architektury przedsiębiorstwa oraz zdefiniowanie procesów biznesowych wraz z systemami wspierającymi umożliwi skuteczne zabezpieczenie systemu sterowania i nadzoru. Spójne zdefiniowanie bezpieczeństwa zasobów teleinformatycznych dla całej organizacji umożliwi z kolei skuteczne zarządzanie bezpieczeństwem i zdefiniowanie go jako proces. Będzie to miało bezpośrednie przełożenie na bezpieczeństwo elementów infrastruktury krytycznej, jakim jest system sterowania i nadzoru. Podejście holistyczne do projektowania architektury systemów w ciekawy, choć trudny do implementacji sposób prezentuje siatka Zachmana. Z racji dynamiki, która cechuje współczesne organizacje, byłoby niezwykle trudno utrzymać ją aktualną. Siatka Zachmana odpowiada nam na pytania (Co?, Jak?, Gdzie?, Kto?, Kiedy?, Dlaczego?) zadane wszystkim uczestnikom procesu tworzenia systemu. Niezależnie od w/w siatki powstał standard SABSA (Sherwood Applied Business Security Architecture). Pierwotnie stworzony do zaprojektowania rozległego systemu finansowego. Jako metodyka skoncentrowana jest na pełnym monitorowaniu przepływu danych, tak aby poziom bezpieczeństwa stawiany systemowi był spełniony. Metodyka opiera się na warstwach, które reprezentują wszystkich uczestników procesu tworzenia architektury bezpieczeństwa. Warstwa operacyjna przechodzi przez pozostałe cztery (kontekstową, koncepcyjną, logiczną, fizyczną) i definiuje bezpieczeństwo w codziennym użytkowaniu.

Czy infrastruktura krytyczna, będzie mniej krytyczna?

Technologia ewoluuje i stawia przed nami coraz to inne wyzwania. Jeżeli uda nam się zdefiniować jednoznacznie model i stosować go przy wdrażaniu i eksploatacji każdego systemu, nie zapominając o obecnie funkcjonujących, mamy szansę być bardziej bezpieczni niż w czasach opisanych na początku tego artykułu. Czerpanie z metodyk, norm, dobrych praktyk opracowanych na potrzeby innych systemów pozwoli nam na budowanie bezpiecznych systemów sterowania i nadzoru, w których dostępność jest tak samo ważna jak poufność czy integralność danych. U progu wykorzystania, również w systemach SCADA, wirtualizacji i cloud computingu, tworzenie sztucznych podziałów (separacji środowisk) jest błędem. Tylko holistyczne podejście do bezpieczeństwa da nam wymierny efekt.

Odpowiadając na pytanie postawione powyżej - **absolutnie nie!** Bezpieczeństwo jest procesem ciągłym i należy traktować je systemowo. Tylko po przez stałe samodoskonalenie (cykl Deminga - PDCA), sprawdzanie poprawności przygotowania przedsiębiorstwa na poziomie organizacyjnym, czy technologicznym, pozwoli nam utrzymać ryzyko na poziomie akceptowalnym. Zauważając zmienność uwarunkowań wynikających z postępu technicznego, wychodząc naprzeciw zdarzeniom gospodarczym, które zwykle wyprzedzają pozostałe, należy dbać o ustawiczne doskonalenie systemów zabezpieczeń kontroli i nadzoru.

Kamil Kowalczuk, absolwent Politechniki Warszawskiej na kierunku Inżynierii Gazownictwa oraz Bezpieczeństwa Systemów Informatycznych na Wydziale Elektrycznym. Generalny Inżynier Bezpieczeństwa IsecMan oraz certyfikowany Ethical Hacker, ITIL® Foundation v.3 oraz Prince2. Pracuje na stanowisku koordynatora w Dziale Bezpieczeństwa Teleinformatycznego w Spółce Operator Gazociągów Przesyłowych Gaz-System S.A.

foto ZBP

BEZPIECZEŃSTWO SYSTEMÓW BANKOWYCH TO POZIOM ŚWIATOWY

Z dr. Mieczysławem Groszkiem, wiceprezesem Związku Banków Polskich rozmawia CIIP focus.

CIIP focus: - Panie Prezesie, czym jest Związek Banków Polskich? Jaka jest jego misja i główne cele?

Mieczysław Groszek: - Związek Banków Polskich to samorządowa organizacja banków, powołana do życia w styczniu 1991 roku. Do zadań statutowych Związku należy reprezentowanie i ochrona wspólnych interesów banków. Misją Związku jest działanie na rzecz tworzenia warunków zrównoważonego rozwoju polskiego sektora bankowego, wspierania przez banki wzrostu gospodarczego kraju oraz jednolitego europejskiego rynku usług finansowych jak również wzmacniania roli polskich banków. Zadania postawione przed Związkiem Banków Polskich wiążą się z zabieganiem o dobre i rozważne regulacje na szczeblu międzynarodowym i krajowym, które mądrze pogodzą troskę o bezpieczeństwo z rozwojem sektora bankowego. Odpowiedzialne rozwiązania podatkowe, sprawność funduszy poręczeniowo-gwarancyjnych, przejrzyste rozwiązania prawne, jak również aktywność na polu absorpcji środków unijnych to kolejne cele, których osiągnięcie stymuluje działania ZBP. Związek uczestniczy w pracach na rzecz kreowania racjonalnych regulacji ostrożnościowych dla sektora bankowego oraz ograniczania nadmiernych obciążeń finansowych banków. ZBP bierze również czynny udział w kształtowaniu regulacji dotyczących systemu bankowego w UE.

- Kogo zrzesza ZBP, a z jakimi podmiotami prowadzi ciągłą współpracę?

- Obecnie członkami Związku Banków Polskich jest 106 banków. Członkostwo w ZBP ma charakter dobrowolny i obejmuje banki działające w Polsce. Z inicjatywy i przy współudziale Związku powstały takie instytucje infrastruktury bankowej, jak: Krajowa Izba Rozliczeniowa S.A., Biuro Informacji Kredytowej S.A. oraz Centrum Prawa Bankowego i Informacji Sp. z o.o. ZBP współpracuje również z Biurem Informacji Gospodarczej InfoMonitor S.A. a także powołał do życia instytucję arbitra bankowego. Związek aktywnie uczestniczy w pracach Rady ds. Systemu Płatniczego przy NBP, Bankowego Funduszu Gwarancyjnego, a także w konsultacjach z Ministerstwem Finansów, Komisjami stałymi Sejmu RP oraz Komisją Nadzoru Finansowego. ZBP reprezentuje także polski sektor bankowy poza granicami kraju, uczestnicząc w pracach Federacji Bankowej Unii Europejskiej, Międzynarodowej Izby Handlowej, Europejskiego Komitetu Standardów Bankowych, Międzynarodowego Stowarzyszenia Bezpieczeństwa Banków oraz Europejskiej Rady ds. Płatności. W ramach Związku i jego biura działa kilkadziesiąt zespołów problemowych, komitetów, rad, komisji i podkomisji, których zadaniem jest opracowywanie i wydawanie opinii oraz stanowisk w sprawach decydujących dla funkcjonowania polskiego systemu bankowego. Pełnią one także rolę integrującą środowisko bankowe wokół wspólnie realizowanych przedsięwzięć.

- Coraz więcej usług bankowych oferowanych jest poprzez Internet. Jakie jest rzeczywiste uzależnienie systemu finansowego (banków) od usług i sieci teleinformatycznych?

W dzisiejszych czasach żyjemy znacznie szybciej niż to miało miejsce chociażby kilkadziesiąt, a nawet kilka lat temu. Mamy coraz mniej czasu, ale za to więcej spraw do załatwienia, również tych związanych z naszą codzienną egzystencją. Dlatego coraz rzadziej odwiedzamy oddziały bankowe i jednocześnie oczekujemy od banków, aby wiele spraw, związanych z naszymi finansami, można było załatwić „na odległość". Dzisiejsza nowoczesna bankowość to nie tylko bankowość internetowa, choć jest to zdalny kanał dystrybucji produktów i usług bankowych nadal najdynamiczniej rozwijających się. Na koniec czerwca 2012 r. liczba klientów mających podpisaną umowę na korzystanie z bankowości on-line wynosiła ponad 19 mln., a liczba klientów aktywnie korzystających z usług on-line to ponad 10,8 mln. Innym dynamicznie rozwijającym się zdalnym kanałem dostępu do usług i produktów bankowych jest bankowość mobilna. Dzięki specjalnym aplikacjom w telefonie komórkowym klienci banków mają dostęp do swojego banku i nie muszą już korzystać z komputerów stacjonarnych, notebooków, netbooków, czy tabletów. Dziś wystarczy, że mamy telefon komórkowy działający w odpowiedniej technologii. Wracając do Pańskiego pytania, bankowość internetowa, czy nawet mobilna nie jest w stanie funkcjonować bez łączności internetowej. Oznacza to, że uzależnienie, o które Pan pyta, jest bardzo duże, choć banki starają się zdywersyfikować ryzyko również w tym obszarze. Z tego względu prowadzone są prace w zakresie rozwoju innych zdalnych kanałów, chociażby wcześniej już wspomnianej bankowości mobilnej, Contact Center lub maszyn samoobsługowych. Takie działania są elementem budowania planów awaryjnych, bo przecież banki jako instytucje zaufania publicznego, muszą nie tylko zapewnić bezpieczeństwo środków zdeponowanych na rachunkach, ale również ich dostępność.

- Czy system bankowy jest bezpieczny przez zagrożeniami teleinformatycznymi? Jaki jest stosunek ZBP do wyzwań w tym zakresie?

Na bezpieczeństwo systemu bankowego składa się wiele elementów, które mogłyby być oddzielnymi tematami naszych rozmów. Zresztą chętnie umówię się na rozmowę na te właśnie tematy. Jeżeli ograniczymy się do bezpieczeństwa w szeroko rozumianej bankowości elektronicznej, to trzeba zwrócić uwagę na dwie kwestie, a mianowicie: bezpieczeństwo systemów bankowych oraz bezpie-

czeństwo klientów korzystających z bankowości elektronicznej. Jeśli chodzi o bezpieczeństwo systemów bankowych, to wyraźnie trzeba stwierdzić, że są one na najwyższym światowym poziomie, czego dowodem jest fakt, że do chwili obecnej nie odnotowaliśmy żadnego skutecznego ataku, który przełamałby stosowane w bankach zabezpieczenia. Inną kwestią jest bezpieczeństwo klientów. Banki nie mają wpływu na to, czy klient posiada: legalne oprogramowanie, zabezpieczenia na komputerze, a jeśli tak, to czy je aktualizuje. Dlatego jako środowisko bankowe podejmujemy szereg innych działań, których celem jest ochrona klienta i jego środków zdeponowanych na rachunkach bankowych z dostępem przez internet. Szkodliwe oprogramowanie infekuje komputery również użytkowników bankowości internetowej. Malware'y te, tworząc komunikaty lub modyfikując strony internetowe banków na zainfekowanych komputerach, kradną tożsamość banku, w celu zasugerowania klientowi, że dane informacje lub prośby są skierowane do niego przez bank. Klient, nie wiedząc, że jest wprowadzany w błąd, przekazuje poufne dane dotyczące identyfikacji i uwierzytelnienia swojej tożsamości oraz autoryzacji transakcji.

- Jakimi metodami osiąga się wspomniany najwyższy, światowy bezpieczeństwa systemu?

Działania sektora bankowego w tym obszarze opierają się na trzech filarach: współpracy pomiędzy bankami, współpracy z organami ścigania i wymiarem sprawiedliwości, edukacji kadry bankowej oraz klientów banków.

W 2009 r. banki uzyskały ustawowe uprawnienie do wymiany pomiędzy sobą informacji objętych tajemnicą bankową, dotyczących przestępstw popełnianych na szkodę banków i ich klientów. W ramach działalności statutowej Związku organizowane są cykliczne spotkania tematyczne przedstawicieli banków, na których omawiane są kwestie związane z bezpieczeństwem elektronicznym.

Od kilku lat odnotowujemy coraz większą efektywność we współpracy z policją, prokuraturą, sądami i Generalnym Inspektorem Informacji Finansowej. Można powiedzieć, że stało się już tradycją organizowanie warsztatów, podczas których bankowcy przekazują swoją wiedzę przedstawicielom organów ścigania i wymiaru sprawiedliwości nt. przeciwdziałania wykorzystywaniu bankowości elektronicznej do celów przestępczych. Jest to bardzo dobra okazja do poznania wzajemnych możliwości i oczekiwań. Ostatnim, równie istotnym jak poprzednie, filarem jest szeroko rozumiana edukacja. Jest ona skierowana zarówno do przedstawicieli banków, dla których Związek organizuje konferencje, szkolenia, seminaria i warsztaty, jak i klientów – użytkowników bankowości elektronicznej. Na stronie internetowej Związku Banków Polskich w dziale edukacja znajduje się informator "Bezpieczny Bank". Można w nim znaleźć informacje jak bezpiecznie korzystać z bankowości internetowej oraz kart płatniczych i jak bezpiecznie kontaktować się z bankiem za pośrednictwem kanału telefonicznego. Można tam również znaleźć aktualne informacje dla klientów banków o najnowszych zagrożeniach dla użytkowników bankowości internetowej.

- Jakie działania podejmuje ZBP w związku z rozwojem technologii informatycznych? Czym jest w strukturze ZBP i jaki jest obszar działania Forum Technologii Bankowych?

Wdrażanie nowoczesnej technologii w bankach nie może się odbywać bez udziału firm technologicznych. Dlatego w ramach Rady Bankowości Elektronicznej Związku Banków Polskich, w dniu 14 kwietnia 2004 r., zostało powołane Forum Technologii Bankowych. Ciało to zrzesza firmy technologiczne współpracujące z bankami i Związkiem Banków Polskich w ramach realizacji zadań statutowych ZBP. Forum jest również propagatorem działań nakierowanych na rozwój gospodarki elektronicznej oraz administracji państwowej i samorządowej wykorzystującej nowoczesne technologie w komunikacji i realizacji spraw z obywatelami. Jak sama nazwa wskazuje Forum jest miejscem wymiany myśli i informacji, jak również edukacji, prezentacji i spotkań z bankowcami w zakresie nowoczesnych technologii i innowacji.

- Jakie są główne obszary działalności FTB? Kto uczestniczy w FTB?

Do Forum należą uznane firmy, liderzy w swoich dziedzinach. Członkowie FTB mają duże osiągnięcia w ramach realizowanych projektów dla banków, jak i podejmowanych inicjatyw na rzecz społeczeństwa informatycznego, a także wzrostu zaufania do bankowości elektronicznej. FTB zrzesza przedsiębiorców posiadających doświadczenia pozytywnie ocenione i zweryfikowane w ramach współpracy z bankami. Główny nurt prac Forum koncentruje się na upowszechnianiu wiedzy o najnowocześniejszych technologiach i ich zastosowaniu w gospodarce elektronicznej, a w szczególności w bankowości. W ramach Forum są tworzone raporty, analizy i opracowania, które inicjują wdrażanie innowacji. Dobrym przykładem prac są dokumenty dotyczące biometrii, identyfikacji i uwierzytelnienia tożsamości, zapewnienia ciągłości działania (BCM). FTB jest zrzeszeniem otwartym na współpracę i promocję rozwiązań korzystnych dla rozwoju polskiej bankowości i gospodarki elektronicznej. FTB współpracuje m.in. z Rządowym Centrum Bezpieczeństwa w zakresie wymiany wiedzy, informacji i doświadczenia, jak również edukacji i promocji obszaru zarządzania ciągłością działania.

- I na koniec, Cloud Computing – czy jest bezpieczny zdaniem ZBP?

Przy Forum Technologii Bankowych funkcjonuje Grupa ds. Cloud Computing. Celem prac grupy jest opracowanie raportu nt. chmury obliczeniowej w sektorze finansowym. Raport zostanie opublikowany na początku 2013 r. Biorąc pod uwagę rozwój technologii i jej ewolucję, ilość przetwarzanych, kumulowanych i gromadzonych danych, chmura to przyszłość. Cloud Computing dynamicznie rozwija się na świecie, plany Komisji Europejskiej zmierzają ku upowszechnieniu tej usługi, a dostawcy zapewniają wysoki poziom bezpieczeństwa. Jednak bezpieczeństwo usług w chmurze budzi największą obawę. Każda nowa technologia, w tym również wspominany model dostarczania usług, wiąże się z pewnymi zagrożeniami. Należy pamiętać, że dane o klientach polskich banków będę przetwarzane poza siedzibą banku, często również poza granicami kraju, co oznacza, że informacje te będą poza kontrolą banków. Dlatego istotnym jest przygotowanie właściwych przepisów prawa, które zagwarantują ochronę danych osobowych oraz informacji objętych tajemnicą bankową. Ważna jest identyfikacja zagrożeń i aktywne im przeciwdziałanie. Pojawia się coraz więcej publikacji i dokumentów dotyczących implementacji tego rozwiązania oraz kwestii ochrony danych i prywatności, mających na celu przyczynienie się do zmniejszenia zagrożeń związanych z wykorzystaniem usług przetwarzania w chmurze.

- Dziękuję za rozmowę.

Skontaktuj się z nami, wyraź opinię, zaproponuj temat – CIIP focus