Informator o ochronie teleinformatycznej

CIP focus

RCB Rządowe Centrum Bezpieczeństwa

www.rcb.gov.pl Maj 2014 nr 7

KOLEJNE PRZEJĘCIE KONTROLI NAD SYSTEMAMI SCADA

Rosyjscy badacze - Sergey Gordeychik i Gleb Gritsai, którzy poświęcili rok 2013 na badania słabości systemów SCADA, odnaleźli słabości, które pozwoliły im na przejęcie kontroli nad wieloma systemami - od paneli słonecznych do systemów transportowych i chemicznych. Słabości dotyczyły systemu Siemens WinCC, takiego samego jak tego używanego w irańskiej elektrowni Natanz, która w 2010 roku została zaatakowana wirusem Stuxnet. Oprócz systemu Siemensa słabość dotyczył również chmurowego rozwiązania SCADA - Daq Connect. Po zgłoszeniu tej słabości w odpowiedzi od właściciela systemu uzyskali odpowiedź, aby "po prostu nie dokonywali ataków".
http://bit.ly/JT3kcD

AMERYKAŃSKIE FIRMY CELEM ATAKÓW SZPIEGOWSKICH

Amerykańskie firmy sekta gazowego i naftowego były celem ataku grupy cyberprzestępczej powiązanej z Federacją Rosyjską. Atakujący dystrybuowali złośliwe oprogramowanie o nazwie HAVEX. W wyniku jego działania informacje o systemie przesyłane są z komputera ofiary do serwera zarządzającego. Wśród nich były również dane autoryzacyjne. Atak nie dotyczył tylko i wyłącznie firm amerykańskich. Atakowane były również kraje z Europy, Bliskiego Wschodu i Azji. Atakowane sektory to m.in. sektory rządowy, obronny, służby zdrowia. Podejrzenia o źródło ataków z Federacji Rosyjskiej wysunęła firma analityczna CrowdStrike, która opublikowała raport dotyczący zagrożenia.
http://bit.ly/1joPXjg

SCADA - INCYDENTY Z BLISKIEGO WSCHODU

Firma SenseCy opublikowała opis kilku ciekawych incydentów dotyczących ataków na systemy SCADA, które swoje źródło miało na Bliskim Wschodzie. Oznacza to, że przeprowadzały go islamskie grupy, a celem ataków były Stany Zjednoczone i ich sojusznicy. W zestawieniu są: atak na stację energetyczną w Kalifornii przeprowadzony przez irańską grupę Parastoo (która ma na koncie włamanie do Międzynarodowej Agencji Energii Atomowej), atak SEA (Syrian Electronic Army) na infrastrukture Izraela oraz atak grupy Jihadist Cyber Terror, która ogłosił rekrutację do cyber-oddziałów, przygotowała listę potencjalnych celów, na której są dostawcy mediów, instytucje finansowe i wielkie korporacje.
http://bit.ly/1jcqetn

*Z **Toomasem Lepikiem** - specjalistą ds. bezpieczeństwa teleinformatycznego w zespole CERT-EE oraz pracownikiem zespołu badawczego w Departamencie Rozwoju Estonian Information Systems Authority, na temat działalności estońskiego zespołu CERT-EE oraz ochrony teleinformatycznej infrastruktury krytycznej w Estonii, rozmawia Mirosław Maj.*

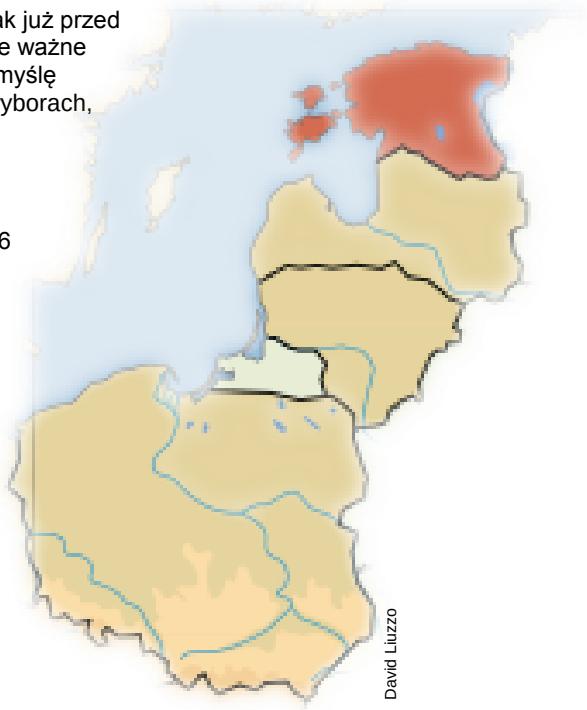
CERT – EE

MM: Toomas, kiedy zespół CERT-EE został stworzony? Czy dobrze pamiętam, że był to rok 2007?

TL: Nie, powstaliśmy rok wcześniej - w 2006.

MM: Kojarzyłem rok 2007, bo wtedy staliście się sławni za sprawą słynnych cyberataków na Estonię.

TL: To prawda. Niemniej jednak już przed tym faktem miały u nas miejsce ważne zdarzenia. Przede wszystkim myślę o drugich w historii Estonii e-wyborach, które miały miejsce w lutym 2007 roku. Mieliśmy ważne zadania związane z zabezpieczeniem teleinformatycznym tego wydarzenia. Już w w 2006 roku ustalone zostało, że w roku 2007 zostanie zwiększony skład zespołu. Wtedy i ja dołączyłem do niego. W naszej historii jest też fragment ścisłej współpracy z wami. W 2008 roku wspólnie pomagaliśmy Gruzji w czasie ataków na ich infrastrukturę teleinformatyczną w czasie wojny z Federacją Rosyjską.



Więcej na str. 2

W numerze:

*Zachęcamy do kontaktu z Redakcją, zgłaszania pomysłów artykułów, tematów, wywiadów: **ciip-focus@rcb.gov.pl***

Z Toomasem Lepikiem - specjalistą ds. bezpieczeństwa teleinformatycznego w zespole CERT-EE oraz pracownikiem zespołu badawczego w Departamencie Rozwoju Estonian Information Systems Authority, na temat działalności estońskiego zespołu CERT-EE oraz ochrony teleinformatycznej infrastruktury krytycznej w Estonii, rozmawia Mirosław Maj.

CERT-EE

Dokończenie ze str. 1

MM: Tak, pamiętam. Kierowałem wtedy zespołem CERT Polska i bezpośrednio wspieraliśmy zespół gruziński, który borykał się z atakami. Byliśmy ich "oknem na świat". Natomiast Wy nawet wysłaliście dwie osoby do Tbilisi, aby pomagały na miejscu.

TL: Tak, dwie osoby pojechały na miejsce do Gruzji. Dodatkowo hostowaliśmy jeszcze gruzińskie serwisy, broniąc je przed cyberatakami.

MM: Jakie inne znaczące zdarzenia były w historii zespołu CERT-EE?

TL: W 2009 roku były następne e-wybory i znowu mieliśmy zadanie je ochraniać. Organizacja zaczęła się rozwijać. Mówię tutaj o całej organizacji o nazwie Estonian Information Systems Authority (RIA - www.ria.ee). Właśnie w jej strukturach w roku 2010 powstał departament zajmujący się bezpieczeństwem teleinformatycznym infrastruktury krytycznej. Zresztą sam zespół CERT-EE również pozyskał nowych członków właśnie wtedy. Jako ośmioosobowy zespól staliśmy się relatywnie dużym zespołem.

W 2011 roku ponownie obsługiwaliśmy wybory. Dodatkowo do naszych zdań operacyjnych doszły regularne działania edukacyjne związane z podnoszeniem świadomości wśród obywateli kraju. Uruchomiliśmy na przykład projekt SFA - Snort for All, który dobrze wpisuje się w te działania (Snort jest jednym z najpopularniejszych darmowych rozwiązań typu IDS - Intrusion Detection System - http://www.snort.org/ - przypomnienie redakcji).

Możemy się również pochwalić tym, że w ramach naszej działalności rozwinęliśmy bardzo popularne wśród zespołów CERT-owych narzędzie jakim jest "Abuse Helper" (http://abusehelper.be/) oraz tzw. Virtual Situation Room (https://www.ria.ee/vsr).

MM: A jak zdefiniowany jest Wasz obszar działania, tzw. constituency?

Z początku działaliśmy jako typowy zespół określany jako "narodowy". Z czasem tendencja była taka, abyśmy byli coraz bardziej odpowiedzialni za infrastrukturę przypisaną do rządu, jego agencji i instytucji. Organizacja, której jesteśmy częścią - RIA - w 2012 roku stała się państwowym regulatorem rynku telekomunikacyjnego. Wtedy też na dobre i w sposób jasny zaczęliśmy być odpowiedzialni za ochronę teleinformatycznej infrastruktury państwa. Jednak było pewne nachodzenie się zakresu odpowiedzialności pomiędzy CERT-EE i Critical Information Infrastructure Unit. Między innymi dlatego doszło do zmian. Został stworzony dokument wyjaśniający zakres odpowiedzialności. Znowelizowane prawo nazywa się "Emergency Act" (https://www.siseministeerium.ee/public/Elutahtsa_teenuste/HOS.pdf). Również macierzysta organizacja CERT-EE – Estonian Informations System Development Center została zreformowana i stworzono Estonian Information System Authority i Critical Information Infrastructure Unit.

MM: Czy jako CERT macie zdefiniowany katalog usług i na jakich warunkach są świadczone?

TL: Nie mamy ściśle określonego zestawu usług. Zresztą w kwestii świadczenia usług problemem jest nie tyle ich katalog co znalezienie odpowiednio przygotowanych partnerów, którzy będą się posługiwali tym samym językiem jak nasi specjaliści i dzięki czemu będziemy w stanie im świadczyć odpowiednie usługi, właśnie w porozumieniu z nimi. Najbardziej pracujemy nad rozwijaniem właśnie takich kontaktów. Oczywiście usługi są również w pewnym stopniu wskazane w dokumencie RFC2350, który opisuje działalność CERT-u (https://www.ria.ee/rfc-2350/).

MM: Jak to działa w konkretnych przypadkach?

TL: Weźmy na przykład ostatni wielki problem jakim jest Heartbleed. To co przygotowaliśmy to szeroka informacja o zagrożeniu oraz rekomendacje dotyczące tego jak sobie radzić z tym problemem.

MM: Skoro jesteśmy przy tym konkretnym zagrożeniu - to czy wykonywaliście testy podatności systemów w Estonii i odnajdywaliście podatne systemy?

TL: Tak, przeprowadzaliśmy takie testy. Nie tylko w domenie rządowej, ale w całym kraju. Przekazywaliśmy informacje do operatorów telekomunikacyjnych. To oni już bezpośrednio kontaktowali się z końcowymi użytkownikami. Zresztą w takiej sytuacji współpracujemy również z wspomnianym Critical Information Infrastructure Unit, jeśli problem dotyczy IK.

Tak naprawdę z jednej strony CERT-EE (Insident Handling Department) w żaden specjalny sposób nie traktuje TIK, ale z drugiej strony bardzo dużą rolę przykładamy do aktywnego wciągania w tematy bezpieczeństwa IT osób odpowiedzialnych za tę infrastrukturę, tak aby byli bardzo dobrze uświadomieni i sami zaczęli systematyczne podnosić poziom bezpieczeństwa tej infrastruktury. Za to jest odpowiedzialna komórka RIA - Cyber Security Branch.

MM: A jak wygląda współpraca publiczna-prywatna w Estonii w kontekście ochrony TIK? Czy to właściciele infrastruktury są w pełni odpowiedzialni za jej bezpieczeństwo? Czy mają konkretne obowiązki?

TL: Właściciele infrastruktury mają oczywiście obowiązki. Przy budowaniu tej współpracy korzystamy z wielu dobrych praktyk wypracowanych samemu (np: ISEKE - https://www.ria.ee/iske-en) jak również powstałych w innych państwach. Wypracowano ważne dokumenty, które również opisują te zasady. Stworzono na przykład "Cybersecurity Strategy" na lata 2008-2013. Jest ona już odnowiona i dotyczy lat 2014-2018. Mamy dokument opisujący wytyczne do przygotowania planów ciągłości działania(https://www.siseministeerium.ee/public/Elutahtsa_teenuste/Toimepidevuse_plaan_EN.pdf), dokument opisujący zasady ochrony IK w regionie państw Morza Bałtyckiego (https://www.siseministeerium.ee/public/Elut_htsate_valdkondade_korraldus_teistes_riikides.pdf), no i rzecz jasna korzystamy z zapisów dyrektywy europejskiej dotyczącej identyfikacji europejskiej infrastruktury krytycznej i oceny potrzeb związanych z jej ochroną (https://www.siseministeerium.ee/public/Direktiiv_Euroopa_esmat_htsate_infrastruktuuride_m_ramise_kohta.pdf).

MM: Zawsze zastanawia mnie sprawa na ile informacja o systemach objętych ochroną i stanowiących TIK, jest informacją poufną? Jak to jest w Estonii?

TL: Tak jak wspomniałem - w "Emergency Act" mamy zdefiniowane serwisy uznane za krytyczne i to jest informacja jawna. Jawne są również zasady kwalifikacji zasobów jako krytyczne, tu oczywiście korzystamy ze wcześniej wspomnianej dyrektywy europejskiej. Nie jest również poufną informacją to czy dane organizacje zarządzają infrastrukturą krytyczną. Natomiast jeśli chodzi o konkretne systemy techniczne, które służą do zarządzania IK to te informacje są niejawne. Czasami oczywiście wiadomo o jakich systemach jest mowa, w szczególności jeśli z pewnych względów stanowią część infrastruktury Internetu. Jednak nawet wtedy informacja o wewnętrznych procesach zachodzących w takich systemach jest chroniona, np: chronione są szczegółowe informacje o konfiguracji urządzeń).

MM: Czy wiadomo ile tego typu systemów jest w Estonii?

TL: 42.

MM: 42? 42 systemy czy organizacje nimi zarządzające?

TL: Nie, 42 serwisy są uznane za krytyczne i one są wymienione w "Emergency Act".

MM: Rozumiem. A czy współpracujecie ze swoimi bliźniaczymi organizacjami z zagranicy?

TL: Głównie robią to przedstawiciele departamentu Critical Information Infrastructure Department (https://www.ria.ee/ciip/). Oni są odpowiedzialni za te zadania. My wspieramy ich głównie w budowaniu kontaktów i wprowadzaniu w relacje z odpowiednimi podmiotami, które sami znamy.

MM: Dziękuję bardzo za te ciekawe informacje i podzielenie się kilkoma wartościowymi materiałami źródłowymi.

TL: Również dziękuję.

BEZPIECZEŃSTWO "INTERNETU RZECZY"

Nieuchronnie nadchodzi era "Internet of Things" (IoT). Dlatego też coraz częściej pojawiają się rozważania na temat bezpieczeństwa tej technologii. Znana organizacja SANS (www.sans.org) przeprowadziła badania na temat obecnego i przyszłego poziomu bezpieczeństwa technologii. W badaniu wzięło udział 391 specjalistów. Wyraźnie widać bliskość technologii IoT i systemów teleinformatycznej IK, np: w obszarze urządzeń HVAC (Heating, Ventilation, Air Conditionning). Dodatkowo pojawia się wiele problemów związanych z bezprzewodowymi systemami medycznymi. Z wyników badania wynika, że specjaliści od bezpieczeństwa już teraz są świadomi czekających ich wyzwań. Wśród nich najczęściej wskazują na dołączenie urządzeń do sieci Internet (50%), kanałami zarządzania urządzeniami (24%) czy bezpieczeństwa systemów jako takich (firmware) (9%). Zapowiadają również to, że będą oczekiwali dojrzałego poziomu bezpieczeństwa od producentów i dostawców urządzeń IoT.
http://www.net-security.org/secworld.php?id=16182

RAPORT NA TEMAT PRZYPADKÓW INCYDENTÓW W AMERYKAŃSKIEJ DOMENIE RZĄDOWEJ

Amerykanie w sposób bezlitosny piętnują przypadki słabej ochrony istotnych zasobów swojego kraju. Raport na ten temat przedstawia incydenty dotyczące takich instytucji jak Komisja Nadzoru Sektora Atomowego, System Powiadamiania Alarmowego, Departamentu Bezpieczeństwa Narodowego czy słynny NIST. W tych i innych instytucjach dochodziło do poważnych uchybień w utrzymaniu bezpieczeństwa systemów, czego powodem były konkretne incydenty związane z wyciekiem informacji czy unieruchomieniem serwisów. Spektakularne ataki znane opinii publicznej to tylko i wyłącznie wierzchołek góry lodowej (ujawniony również poprzez działalność cyberprzestępców). "Pod wodą" pozostają dziesiątki tysięcy nieznanych incydentów. Od 2006 roku Amerykanie wydali na zabezpieczenie systemów administracji rządu federalnego co najmniej 65 miliardów dolarów.
http://www.coburn.senate.gov/public/index.cfm?a=Files.Serve&File_id=f1d97a51-aca9-499f-a516-28eb872748c0

Cyber-EXE Polska 2013 za nami

Czas na podsumowania, wnioski i rekomendacje - cd.

Maciej Pyznar

Rządowe Centrum Bezpieczeństwa

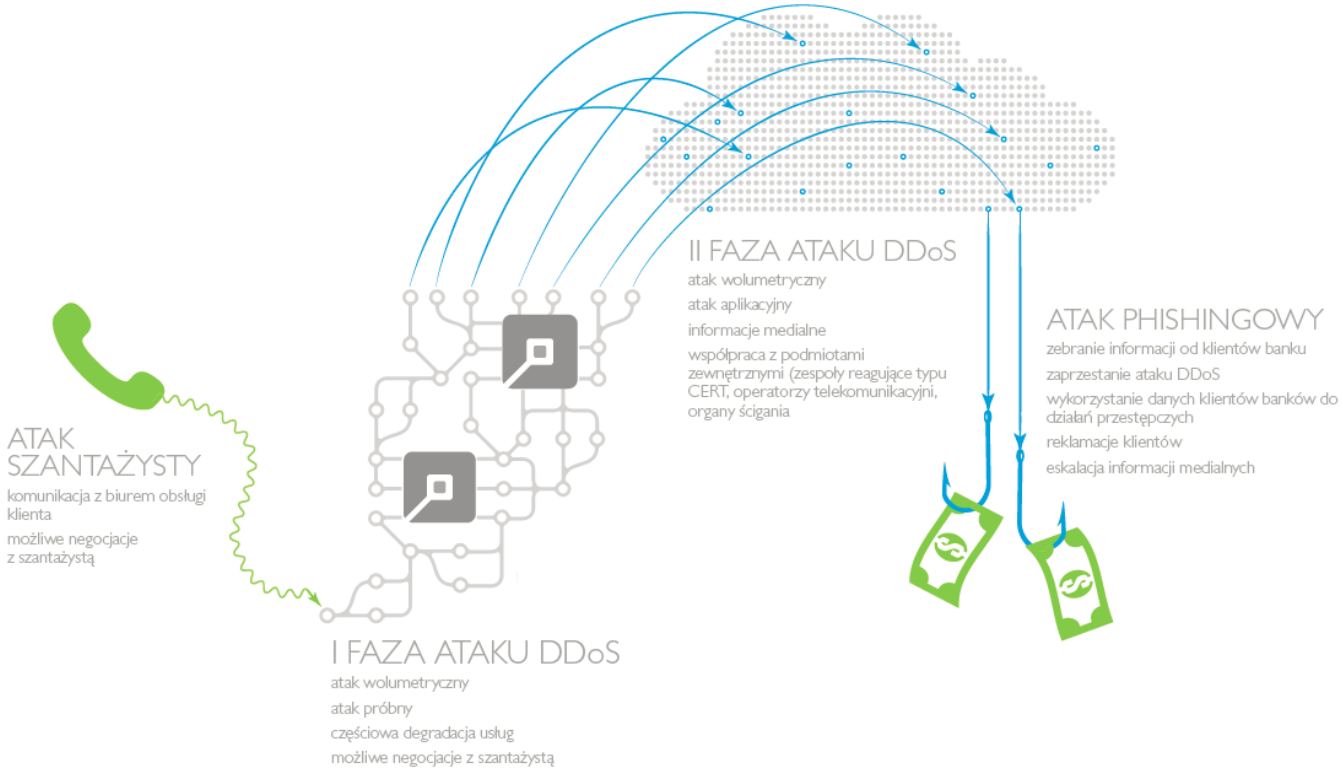
Mirosław Maj

Fundacja Bezpieczna Cyberprzestrzeń

W poprzednim artykule na temat ćwiczenia Cyber-EXE Polska 2013 (CIIP Focus nr 6) opisaliśmy cele ćwiczenia, modele jego przeprowadzenia oraz przekazaliśmy garść informacji na temat jego organizacji i tego, co działo się 29 października 2013 roku w Centrum Koordynacji Ćwiczenia.

Teraz nadszedł czas by uchylić rąbka tajemnicy dotyczącego scenariusza i przedstawić najważniejsze wnioski i rekomendacje z ćwiczenia.

Scenariusz składał się z dwóch wątków. Pierwszy z nich to atak DDoS, zaś drugi to dedykowany atak na wrażliwe dane klientów i pracowników banków, który był odpowiednikiem ataku wykonanego zgodnie z typowym scenariuszem towarzyszącym atakowi typu APT (Advanced Persistant Threat). Pierwszy wątek scenariusza ilustruje poniższy rysunek.



Wątek scenariusza ćwiczenia przedstawiający atak typu DDoS

Szantażysta, w którego wcielił się moderator główny ćwiczenia, poinformował biuro obsługi klienta, że jeśli nie zostaną spełnione jego żądania, przeprowadzi atak DDoS na witryny internetowe banku. Założeniem było, by moderator główny prowadził negocjacje w ten sposób, żeby zostały one zerwane. Tylko wtedy szantażysta mógł przeprowadzić kolejne fazy ataku, a na koniec spróbował przechwycić dane autoryzacyjne klientów banków do serwisów transakcyjnych, czyli zrealizować całość zamierzonego scenariusza, a tym samym możliwe było sprawdzenie reakcji banków na wszystkie elementy ataku. Zadanie ćwiczących polegało przede wszystkim na działaniach minimalizujących skutki ataku oraz przywróceniu normalnej funkcjonalności serwisów internetowych. W tej części, uczestnicy koncentrowali się na sprawdzeniu istniejących procedur pod kątem ich poprawności i przydatności w ćwiczonej sytuacji. Na marginesie warto dodać, że zespół odpowiedzialny za właściwą moderację negocjacji z szantażystą, sprawnie odrzucał wszelkie propozycje, a reakcje niektórych ćwiczących były raczej potwierdzeniem faktu, że banki nie wchodzą w poważne negocjacje z przestępcami.

Wątek scenariusza ćwiczenia przedstawiający atak typu APT

Drugim wątkiem ćwiczonym podczas Cyber-EXE Polska 2013, był atak dedykowany. Zgodnie z tym scenariuszem, na początku w mediach pojawiły się fragmenty poufnych informacji bankowych (polityka wobec konkurencji, dane teleadresowe członków zarządu). Następnie, podobnie jak w wątku DDoS, nastąpił atak. Zadaniem ćwiczących było znaleźć źródło wycieku informacji. Działanie to odbywało się pod presją czasu, gdyż szantażysta co pewien okres czasu, za pośrednictwem mediów, publikował coraz wrażliwsze informacje dotyczące ćwiczących banków. Każdy z uczestników, w odpowiedzi na diagnostykę swoich systemów teleinformatycznych (wyniki tej diagnostyki symulował moderator główny), otrzymywał pakiet informacji, wśród których znajdowała się również wskazówka pozwalająca dotrzeć do sprawcy ataku. Kilka z takich „puzzli" zostało przekazanych ćwiczącym bankom. Celem takiego działania było zachęcenie banków do wzajemnej wymiany informacji. Jeśli tak by się stało, puzzle miały utworzyć „obrazek" w łatwy sposób pozwalający namierzyć atakującego. Niestety, nie doszło do wystarczająco intensywnej wymiany informacji, która zgodnie z przyjętymi zasadami pozwoliłaby na „rozwiązanie zagadki".

Warto przy tym zaznaczyć, że ćwiczenia oprócz warstwy operacyjnej prowadzone były również w warstwie medialnej – wydarzenia zaplanowane w scenariuszu miały swoje odzwierciedlenie w symulowanym „świecie mediów". Zrealizowane zostało to przy pomocy specjalnie przygotowanej internetowej strony komunikacji medialnej udostępnionej przez RCB. Strona składała się z dwóch części. W pierwszej ukazywały się informacje, które w sytuacji realnej byłyby przekazywane przez media (TV, radio, prasa, agencje informacyjne, portale internetowe i portale społecznościowe). Za informacje na tej części platformy odpowiadała, usytuowana przy moderatorze głównym ćwiczenia, grupa symulująca pracę mediów (osoby, które w trakcie ćwiczenia „udawały" dziennikarzy). W drugiej części strony internetowej służby prasowe/PR banków prezentowały swoje komunikaty i informacje oraz wszelką aktywność medialną w związku z sytuacją kryzysową. Na stronie komunikacji medialnej próbki skradzionych informacji publikował także szantażysta, ważnym zatem elementem ćwiczenia była wewnętrzna komunikacja pomiędzy służbami prasowymi/PR banków i zespołami ćwiczącymi w warstwie operacyjnej. To dodatkowo powodowało założone w scenariuszu „przeciążenie" ćwiczących. Trzeba przyznać, że ćwiczenia w warstwie medialnej stanowiły niezwykle realistyczny fragment ćwiczenia i w intensywny sposób zaangażowały uczestników po stronie banków. Jak poradziły sobie z tym wszystkim ćwiczące banki? Nad wyraz dobrze.

Pierwszy i najważniejszy wniosek jaki nasunął się po zakończeniu ćwiczenia jest następujący: czynnikiem, który miał decydujący wpływ na rozwiązanie symulowanej sytuacji kryzysowej, był niezwykle kompetentny personel. Zaobserwowaliśmy, że u wszystkich uczestników Cyber-EXE Polska 2013 funkcjonują procedury obejmujące swoją treścią większość sytuacji przewidzianych w scenariuszu ćwiczenia. Mnogość współcześnie występujących zagrożeń wymusza maksymalne uproszczenie procedur, inaczej liczba koniecznych procedur uniemożliwiałaby ich skuteczne użycie. Dlatego tak dużą rolę odgrywa w tej sytuacji doświadczenie osób uczestniczących w reagowaniu, ich kreatywność i osobiste zaangażowanie oraz zdolność do koordynacji działań w sytuacjach kryzysowych. Niezwykle istotne jest zatem, by utrzymać wiedzę osób odpowiedzialnych za reagowanie na najwyższym możliwym poziomie. Inwestycja w tę wiedzę powinna być poważna. Personel odpowiedzialny za te zadania powinien mieć pełen dostęp do wiedzy (np. subskrypcja na branżowych portalach internetowych) oraz szkoleń w tym zakresie. Szkolenia powinny dotyczyć nie tylko osób bezpośrednio odpowiedzialnych za bezpieczeństwo teleinformatyczne, ale również wszystkich pracowników, których nieprawidłowe działanie może istotnie wpłynąć na poziom bezpieczeństwa w banku.

Drugą ważną obserwacją, jest duża zależność banków od podmiotów zewnętrznych. W obszarze teleinformatycznym są to przede wszystkim operatorzy telekomunikacyjni. W praktyce, ich udział w rozwiązaniu problemu jest kluczowy w sytuacji, kiedy trudno sobie wyobrazić skuteczną reakcję bez ich wsparcia lub chociażby koordynacji z nimi. Tak jest na przykład w sytuacji ataku typu DDoS.

Kolejny istotny wniosek dotyczył współpracy pomiędzy bankami, która miała prowadzić do sprawniejszego rozwiązania problemu. Taka współpraca w czasie ćwiczenia była prowadzona, aczkolwiek w podstawowym zakresie. Jest to z pewnością zadanie na przyszłość – tj. ustalenie jak taka współpraca powinna wyglądać. Wydaje się, że najistotniejsze sprawy, które powinny być rozstrzygnięte, to ustalenie czy ta współpraca jest postrzegana jako konieczna i w jakim zakresie jest realna. Jeśli to zostanie ustalone, to pozostanie stworzenie odpowiednich ram współpracy formalnej, tak aby pracownicy banków nie mieli wątpliwości co do tego jaką informacją mogą się dzielić, a jaką nie. W pracach nakierowanych na rozwój współpracy między bankami warto wziąć pod uwagę przestrzeń stworzoną przez ZBP do przeciwdziałania atakom na bankowość elektroniczną, w tym możliwość prowadzenia wspólnej polityki informacyjnej i koordynacji działań.

Przytoczone wnioski to tylko niektóre z całego zestawu. W raporcie z ćwiczenia (Raport z ćwiczenia Cyber-EXE Polska 2013 do pobrania ze strony www.cyberexepolska.pl) znajduje się pełen zestaw wniosków zgrupowanych w działy dotyczące działań wewnętrznych banków, całości sektora bankowego, komunikacji medialnej i organizacji ćwiczeń. Wszystkim wnioskom towarzyszą odpowiednie rekomendacje. Zachęcamy do zapoznania się z całym zestawem.

TWOJA SCADA DOSTĘPNA z INTERNETU

Mirosław Maj

WODNE WOJNY w STANIE ILLINOIS

W listopadzie 2011 roku pracownik stacji pompowania wody w stanie Illinois w USA badał przyczyny awarii urządzeń odpowiedzialnych za działanie całej stacji. Przeglądał on logi systemowe urządzenia typu SCADA, które odpowiadało za kontrolę i sterowanie pompami wodnymi. W trakcie tego badania dokonał dość szokującego odkrycia. Wykrył, że pięć miesięcy wcześniej do systemu logował się użytkownik, który łączył się do niego z Rosji!

Atmosfera wokół odkrycia była coraz bardziej napięta. Lekko przypominała tę pokazaną w filmie z 1983 „Gry wojenne", kiedy narastało napięcie pomiędzy USA i Związkiem Radzieckim. Sytuacja nie tak poważna jak w fabule filmu, ale wniosek nie był fikcyjny – połączenie było z rosyjskiego IP - system zaatakowali rosyjscy cyberprzestępcy.

Zarządzający stacją przekazali informację do Agencji Ochrony Środowiska (Environmental Protection Agency) a pracownicy Agencji do Centrum Wywiadu i Ochrony przed Terroryzmem dla Stanu Illionois. W Centrum nad sprawą pochylili się pracownicy policji stanowej, FBI i Departamentu Bezpieczeństwa Narodowego. 10 listopada wydano oficjalne oświadczenie, w którym informowano o „cyberwłamaniu do systemu dostawy wody". 16 listopada sprawa trafiła do federalnego zespołu CERT-owego od spraw ochrony infrastruktury krytycznej – ICS-CERT, który przystąpił do dalszej analizy przypadku, który coraz bardziej wyglądał na atak na infrastrukturę krytyczną Stanów Zjednoczonych. 23 listopada ICS-CERT opublikował oficjalną notatkę na temat incydentu.

Cała sprawa okazała się banalna. Za „włamaniem" stał pracownik firmy obsługującej stację, który połączył się zdalnie z systemem zarządzania, wprost ze swojego komputera. Pech polegał na tym, że w tym czasie pracownik przebywał na wakacjach w Rosji i korzystał z usług rosyjskiego operatora telekomunikacyjnego, miał więc przypisany „rosyjski" numer IP.

Ta sytuacja, która wydawała się poważna, później krytyczna, a na koniec raczej zabawna, pokazuje jednak jeden bardzo istotny problem związany z zarządzaniem systemami kontroli przemysłowej – systemy te bardzo często dostępne są w sposób zdalny z Internetu, co wystawia je na potencjalnie dość duże niebezpieczeństwo. Praktyka jest prosta. Systemy SCADA bardzo często są obsługiwane z wykorzystaniem usług firm trzecich, które sprawują nad nimi usługi serwisowe. Firmy te, aby minimalizować koszty takiej usługi pozostawiają możliwość zdalnego dostępu do systemu. Jest to tańsze i łatwiejsze. Dzięki temu pracownik może obsługiwać system ze swojego biura, z domu, a nawet jak widać po opisanym przypadku – w czasie wakacji w obcym państwie.

PROJEKT SHODAN

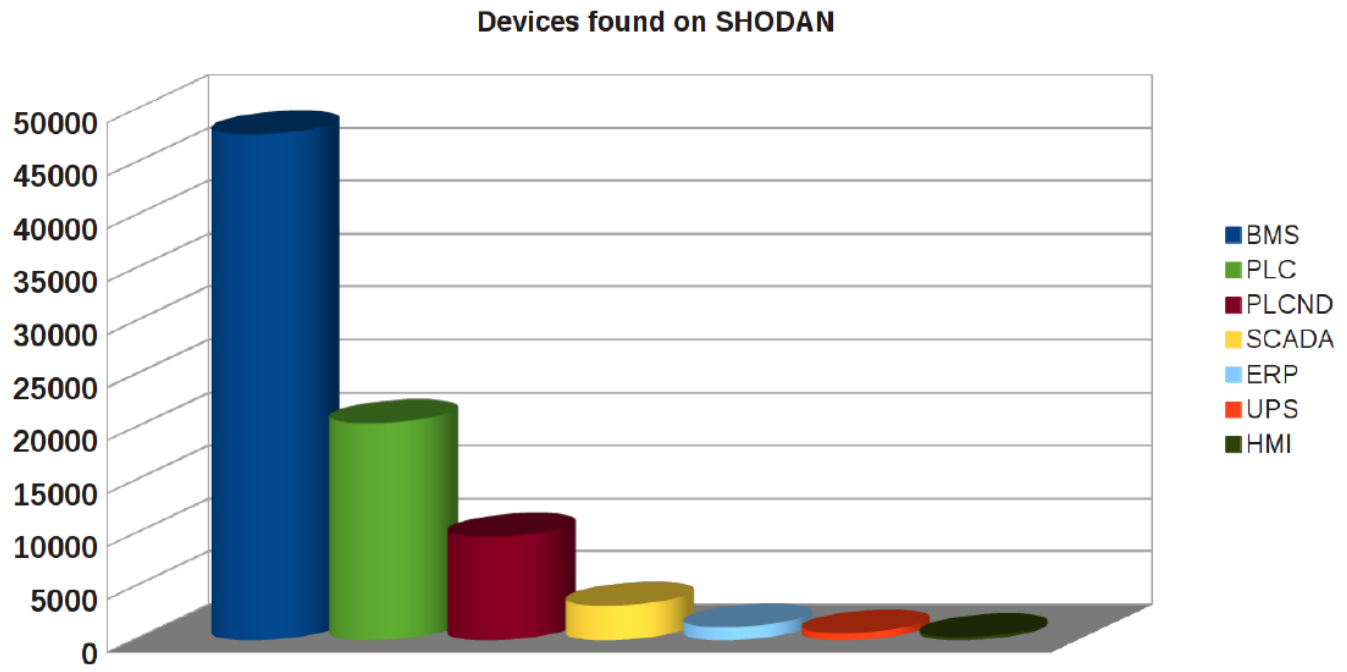
Czy takich systemów jest dużo? Trudno jednoznacznie powiedzieć. Są jednak istotne przesłanki, aby odpowiedzieć na takie pytanie twierdząco. Chyba najważniejszego argumentu za taką odpowiedzią dostarcza projekt Shodan. Czym jest Shodan? To projekt polegający na uruchomieniu wyszukiwarki dostępnej online, która pozwala na wyszukanie urządzeń sieciowych takich jak rutery, serwery, kamery internetowe jak również systemy zarządzania przemysłowego. Projekt rozpoczął w 2009 roku John Matherly. Korzystający z wyszukiwarki, po przygotowaniu precyzyjnego zapytania, może dość dokładnie wyszukać interesujące go urządzenia i odnaleźć je w sieci, a następnie się do nich połączyć. Jeśli są źle zabezpieczone, np.: używają domyślnych haseł ustawionych przez producenta, to w bardzo łatwy sposób można do tych systemów uzyskać dostęp. Co można później zrobić? Bardzo różne rzeczy – w zależności od poziomu praw dostępu nawet te najgorsze z punktu widzenia właściciela systemu, np.: może wyłączyć urządzenie, albo co czasami gorsze – zmienić parametry jego działania. Przykłady konsekwencji praktycznych takich zaniedbań lepiej nie przywoływać, żeby nie straszyć. Specjaliści od systemów sterowania wiedzą jakie operacje są możliwe z wykorzystaniem tych systemów i jakie może to rodzić konsekwencje.

Popular Tags	
webcam	58
scada	48
http	39
camera	38
router	38
cam	34
ftp	34

Najpopularniejsze zapytania w systemie Shodan

PROJEKTY OPARTE NA SHODAN

Projekt Shodan stał się inspiracja dla wielu badaczy sprawdzających bezpieczeństwo systemów typu SCADA. Wyszukiwanie systemów SCADA stało się jednym z najczęstszych zapytań w wyszukiwarce.
Dwóch badaczy z firmy InfraCritical – Bob Radvanovsky i Jacob Brodsky przeprowadzili badania, w wyniku których zidentyfikowali 7 200 urządzeń, które pochodziły z listy kluczowych zasobów dostarczonej przez Departament Bezpieczeństwa Wewnętrznego USA, a które udostępniały w sieci interfejsy do wprowadzenia loginu i hasła do systemu. Biorąc pod uwagę jak często te loginy i hasła są po prostu domyślnymi hasłami dla poszczególnych typów urządzeń, to łatwo sobie wyobrazić, jakie mogą być konsekwencje takiej dostępności. Badania wskazują, że w około 15% przypadków to co jest znalezione przez wyszukiwarkę Shodan kończy się możliwością praktycznego dostępu do zarządzania systemem. Badacze z InfraCritical odnaleźli w ten sposób urządzenia do sterowania systemem dostawy wody, energii, wentylacji i ogrzewania, maszyn górniczych, kontroli ruchu drogowego, a nawet krematoriów, co należałoby uznać za przejaw „czarnego humoru". Całość obejmował urządzenia należące do 70 różnych producentów.
Innym ciekawym projektem jest prowadzony przez uczonych z Frei Universitat w Berlinie projekt SCADA CS. Stworzyli oni mapę dostępnych urządzeń typu ICS (Industrial Control System), które są widoczne z publicznej sieci Internet (Industrial Risk Assessment Map (IRAM)). Są wśród nich popularne klasy urządzeń takie jak: ERP (Enterprise Resource Planning), HMI (Human Machine Interface), PLC (Programmable Logic Controller), SCADA (Supervisory Control And Data Acquisition), UPS (Uninterruptible Power Supply)



Urządzenia znalezione w wyszukiwarce Shodan w ramach projektu SCADA CS (źródło)

Aktywności, inicjatyw i projektów związanych z wyszukiwaniem publicznie dostępnych urządzeń ICS i badaniem ich podatności jest bardzo dużo. Można przywołać tu badanie przeprowadzone przez dwóch pracowników Kaspersky Lab – Terrego McCorkle i Billego Riosa, którzy w 2011 roku przedstawili wyniki swojego projektu „100 bugs in 100 days". W jego ramach znaleźli 665 słabości systemowych w 76 systemach HMI z 380, które odnaleźli. 75 z tych słabości pozwalały na włamanie do systemu.

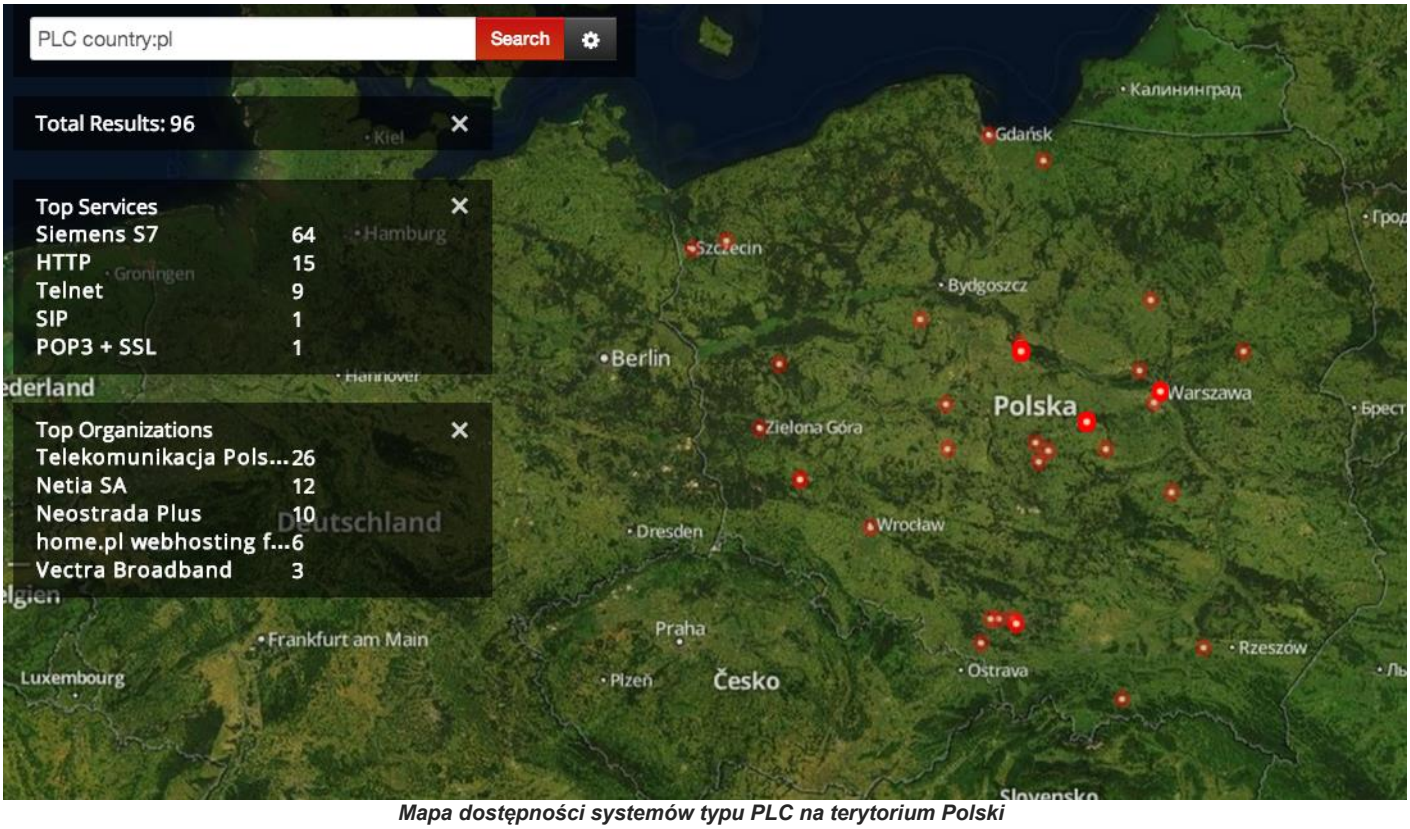
A JAK JEST w POLSCE?

Czytając te niepokojące doniesienia ze świata od razu przychodzi na myśl pytanie jak wygląd sytuacja w Polsce? Rzetelna odpowiedź wymaga z pewnością większego przedsięwzięcia – być może podobnego do jednego z tych, które są opisane powyżej. Niemniej jednak kilka prostych sprawdzeń już wskazuje na fakt, że wynik poszukiwań systemów, które narażone są na ataki z zewnątrz, nie będzie zbiorem pustym. Przeprowadziliśmy sprawdzenie dotyczące dostępnych urządzeń obsługujących kilka dość popularnych systemów dla środowiska teleinformatycznej IK. Wyniki takich sprawdzeń zamieszczamy poniżej.

Mapa dostępności systemów Simatic na terytorium Polski

„Mapa dostępności systemów Simatic na terytorium Polski" pokazuje między innymi istnienie urządzeń Siemens S7. Urządzenie to jest tzw. kontrolerem PLC, które jest jednym z najbardziej popularnych urządzeń w swojej klasie. Proste wyszukiwanie wskazało na możliwość dostępu do 26 urządzeń tego typu. Dla porównania, analogiczne wyniki dla Niemiec, Francji, Czech i Rosji wynoszą odpowiednio: 137, 34, 26 i 20.

Co ciekawe, powyższe wyszukanie wcale nie pokazuje kompletnej listy dostępnych systemów. Nieraz uzyskanie informacji o większym zbiorze związane jest z eksperymentami w ustawianiu składni zapytań. Wiedząc, że system Siemens S7 jest sterownikiem PLC można dokonać zapytania właśnie dotyczącego PLC. W tym przypadku otrzymujemy informację o dostępności w Polsce aż 64 systemów tego typu.



Mapa dostępności systemów typu PLC na terytorium Polski

Bezpieczeństwo inteligentnych sieci energetycznych

Mirosław Maj

ENISA (European Information Security Agency) opublikowała kolejny materiał, który możemy zaliczyć do zestawu publikacji dotyczących bezpieczeństwa teleinformatycznej infrastruktury krytycznej. Dokument nosi nazwę "Smart Grid Threat Landscape and Good Practice Guide". To kontynuacja wysiłków Agencji skierowanych na zwiększenie wiedzy dotyczącej zagrożeń, w szczególności tych specyficznych, dotyczących IK. Zresztą autorzy nawiązują do doświadczeń nabytych przy tworzeniu publikacji "ENISA Annual Incident Report 2012"[1], o których pisaliśmy w jednym z poprzednich numerów CIIP focus.

Co zawiera dokument ENISA i dla kogo powstał?

Tym razem, jak wskazuje na to tytuł, na warsztat wzięto inteligentne sieci energetyczne (dalej: ISE), popularnie nazywane "smart grid". Materiał stanowi ciekawe narzędzie dla właścicieli lub odpowiedzialnych za bezpieczeństwo ISE, którzy wśród swoich zadań mają zadania związane z analizą zagrożeń, oceną ryzyka i wypracowaniem sposobów jego mitygacji. Oprócz praktyków i tych, na których spoczywają zadania natury operacyjnej, materiał Enisy może być również przydatny dla osób odpowiedzialnych za wypracowywanie regulacji dotyczących tej tematyki. Otrzymują oni do swych rąk materiał, w którym znajduje się usystematyzowana wiedza na temat obecnych trendów związanych z zagrożeniami dla ISE. Bez tej wiedzy trudno sobie wyobrazić powstawanie skutecznych regulacji lub chociażby wewnątrzorganizacyjnych materiałów określających sposób zarządzania bezpieczeństwem ISE.

Co ciekawego można odnaleźć w dokumencie?

Opracowanie ENISA powinno być szczególnie ciekawe dla osób zajmujących się problematyką cyberzagrożeń. Oczywiście nie brakuje w nim usystematyzowanej wiedzy na temat wszystkich zagrożeń (np: dotyczących bezpieczeństwa fizycznego - tak istotnego w przypadku ochrony IK), ale to właśnie element teleinformatyczny został najdokładniej „rozpracowany". Autorzy wychodzą z założenia, że w związku z szerokim wykorzystaniem technologii IT w sieciach energetycznych, właśnie ten aspekt powinien być dokładnie przedyskutowany. Najwyraźniej chcą w ten sposób wzbogacić literaturę dotyczącą zagrożeń dla sieci energetycznych właśnie o aspekt cyberbezpieczeństwa.

Zasoby oraz zagrożenia ich dotyczące

Aby ustalić katalog zagrożeń trzeba pracę rozpocząć od ustalenia listy zasobów, których te zagrożenia mogą dotyczyć. Tutaj autorzy dostarczyli wartościowego „gotowca". Może on być bezpośrednio skonfrontowany z listą własnych zasobów lub wręcz posłużyć do stworzenia takiej listy. Główne zasoby wykazane przez ENISA to: sprzęt, infrastruktura, zasoby ludzkie, zasoby typu e-mobility, usługi, oprogramowanie, informacja. Z pewnością analityk doszukałby się w tym podziale pewnych błędów metodycznych, np. sprzęt może również stanowić część infrastruktury, a nawet wyposażenia z grupy e-mobility, które stanowić może wg autorów np. stacja ładowania energią dla pojazdów elektrycznych. Wydaje się więc, że autorzy postawili przede wszystkim na podział praktyczny. Takie praktyczne podejście pozwala też wychwycić najłatwiej te grupy zasobów, które są najistotniejsze dla badacza tematyki cyberbezpieczeństwa. Wśród nich są: sprzęt typu "smard grid", na przykład zdalne terminale czy sterowniki PLC, sprzęt "kliencki" typu komputer, laptop czy drukarka, sprzęt sieciowy, taki jak switche czy modemy (jak wiadomo nadal dość powszechnie wykorzystywane w zarządzaniu infrastrukturą krytyczną). Oprócz powyższych, praktycznie w pewnym stopniu wszystkie pozostałe elementy, choć częściowo dotyczą również bezpieczeństwa teleinformatycznego.

Skoro mamy już zestawienie zasobów, to można przypisać im odpowiednie zagrożenia. Katalog tych zagrożeń to bardzo pożyteczna i praktyczna część dokumentu. Stanowi doskonały punkt wyjścia dla analizy ryzyka własnych zasobów. ENISA zaproponowała 7 grup zagrożeń: intencjonalny atak fizyczny, nieintencjonalne zniszczenie danych, awarie, przejęcie danych w wyniku podsłuchu lub przejęcia komunikacji, naruszenia prawa, umyślne działanie na szkodę, zaniki dostawy energii, zniszczenie lub utrata zasobów IT, katastrofy naturalne.

Każda z tych grup jest w dokumencie szczegółowo opisana, dlatego jeśli pojawiają się jakiekolwiek wątpliwości dotyczące zakresu definicji dla poszczególnych grup, można je niezwłocznie wyjaśnić. Jest z czym się zapoznawać. Katalogi obejmują od trzech podkategorii dla prawnych zagrożeń, aż po 22 pozycje dla zagrożeń określonych jako "umyślne działanie na szkodę".

Na koniec tej części opracowania, tj. powiązania pomiędzy zasobami i zagrożeniami, autorzy przedstawiają czytelnikowi tabelę, w której dla każdej pozycji związanej z zagrożeniem wskazane są zasoby, których to zagrożenie może dotyczyć. Takie zestawienie to kolejny krok w kierunku przygotowania prawie gotowej, uniwersalnej matrycy, która może posłużyć do przygotowania analizy ryzyka.

Powyższa analiza wskazuje, że tak naprawdę słabości zasobów ISE nie są szczególnie inne niż te dotyczące innych systemów teleinformatycznych. W chwili obecnej trudno jest jednoznacznie odpowiedzieć na pytanie czy rozpoznany katalog zagrożeń jest pełny i nic w nim nie umknęło. Tak naprawdę dopiero pojawiają się projekty (niektóre z nich są w realizacji) traktujące tę problematykę. Autorzy wskazują na kilka ciekawych projektów z tej dziedziny.

Pierwszy z nich to projekt n-Shield [2]. Obejmuje on kwestie bezpieczeństwa, prywatności i zależności w kontekście systemów wbudowanych (ang. embeded systems) takich zasobów jak kolej czy lotnictwo, to jednak podobnie jak w ISE, sprawa dotyczy IK i w praktyce, systemów o podobnej architekturze i przeznaczeniu.

Drugi z wymienionych projektów to nie tyle projekt co właściwie cały program badawczy stworzony przez Komisję Europejską (DG Home Affairs) poświęcony tematyce terroryzmu i innych ryzyk dla bezpieczeństwa. (Terrorism & other Security-related Risks (CIPS))[3].

Wreszcie ostatni projekt to Crisalis Project [4]. Crisalis jest projektem dotyczącym wypracowania narzędzi do ochrony IK przed dedykowanymi atakami. Jako przykłady ataków dedykowanych i zaawansowanych autorzy projektu podają Stuxneta i Duqu.

Źródła zagrożeń

Posiadanie listy i opisów zagrożeń i zasobów to doskonały materiał wyjściowy dla analityków ryzyka. Analogicznie do tego, w opracowaniu można odnaleźć bardzo dobry materiał dla tych, którzy są w organizacjach odpowiedzialni za przygotowanie planu minimalizacji lub likwidacji wybranych ryzyk. Wiadomo, że aby to dobrze zrobić, potrzebna jest możliwie najbardziej szczegółowa wiedza na temat źródeł zagrożeń. W opracowaniu autorzy zaproponowali 8 typów takich źródeł, zdecydowanie koncentrując się na osobowym ich charakterze, z wyłączeniem źródła katastrof naturalnych, którymi po prostu są... katastrofy naturalne.

Oto jakie zostały wyróżnione źródła zagrożeń i jakie są najbardziej charakterystyczne cechy tych źródeł:

- korporacje - wyróżniają je taktyki ofensywne, walka o przewagę konkurencyjną. Zagrożenia realizowane przez to źródło to wynik skoordynowanych działań technicznych i socjotechnicznych;
- cyberprzestępcy - działający głównie z motywacją zysków finansowych, bardzo często operujący w zorganizowanych grupach przestępczych, mają korzenie krajowe lub międzynarodowe;
- pracownicy - zatrudnieni bezpośrednio w organizacjach lub w wyniku umów i kontraktów. Bardzo często na stanowiskach związanych z teleinformatyczną lub fizyczną ochroną zasobów;
- haktywiści - atakujący, których motywacje są najczęściej polityczne lub społeczne. Stawiają sobie dość ambitne cele, dlatego często ich ataki dotyczą bardzo istotnych zasobów;
- państwa - specjaliści lub całe oddziały, które zostały przećwiczone do przeprowadzania ataków. Powszechną już bronią w ich arsenale są narzędzia ofensywne;
- zagrożenia naturalne (brak powiązania z elementami cyberzagrożeń);
- terroryści - mogą również przeprowadzać cyberataki. Ich motywacje są polityczne lub religijne, natomiast "siła rażenia" jest bardzo zróżnicowana i zależy od determinacji oraz posiadanych środków;
- cyber-wojownicy - mniej lub bardziej zorganizowane grupy patriotyczne zaangażowane w konflikty międzynarodowe. Ich motywacje są podobne do motywacji terrorystów - polityczne i religijne. Ich działalność jest niekiedy wspierana (w tym organizacyjnie i finansowo) przez czynniki państwowe.

Podobnie jak w przypadku zasobów i zagrożeń, gdzie autorzy przedstawili powiązania pomiędzy tymi dwoma obszarami, tak i w przypadku katalogu źródeł również jest materiał syntetyczny. Tym razem pokazano relacje pomiędzy zagrożeniami a ich źródłami. Analitycy mogą z pomocą zamieszczonej w raporcie tabelki zidentyfikować, które ze źródeł zagrożenia jest najbardziej prawdopodobne w przypadku poszczególnych zagrożeń. Ujmując sprawę ilościowo wychodzi na to, że najbardziej prawdopodobnym źródłem zagrożenia jest pracownik organizacji. Ten typ zagrożenia nie pojawia się tylko w przypadku dwóch rodzajów zagrożeń - ataku fizycznego i zniszczenia zasobów (choć jak chwilę się zastanowić to być może i dla tych kategorii pracownik mógłby stanowić źródło zagrożenia). Innymi bardzo prawdopodobnymi źródłami są inne państwa i terroryści. Natomiast stosunkowo najmniej zagrożeń należy się obawiać ze strony korporacji i katastrof naturalnych.

Najlepsze praktyki, czyli co robić.

Wskazanie zasobów, zagrożeń i ich źródeł to materiał bardzo ciekawy i użyteczny. Niemniej jednak najbardziej użyteczna część całości opracowania to oczywiście propozycji najlepszych praktyk w dziedzinie ochrony ISE.
Podejście, które przestawiono w raporcie to koncentracja na propozycjach zabezpieczenia w odniesieniu do dwóch najważniejszych grup - systemów teleinformatycznych i sieci logicznych wykorzystanych w ISE oraz tzw. "łańcucha dostaw", który uwzględnia bezpieczeństwo producentów rozwiązań, dystrybutorów i użytkowników końcowych.

W kontekście prezentacji najlepszych praktyk raport ENISA jest de facto tylko katalogiem haseł związanych z tymi praktykami oraz zestawieniem materiałów referencyjnych, które mogą posłużyć do zapoznania się, oceny i ewentualnej implementacji takich praktyk. Rozdział o nazwie "IT Systems and Logical Networks" zawiera 45 pozycji, a każda z nich odsyłacze do zazwyczaj jednej lub dwóch (czasami kilku) dobrych praktyk, mówiących o tym jak osiągnąć pożądany poziom bezpieczeństwa. Na przykład pkt 12 - "Stworzenie systemu monitoringu incydentów 24/7, uwzględniającego logowanie zdarzeń i audyt systemów" ma odsyłacze do dwóch pozycji:
"Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure" [5] oraz
Utility Cyber Security - Seven Key Smart Grid Security - Trends to Watch in 2012 and Beyond.

Ten przykład to tylko fragment bardzo dużej części opracowania, które stanowi chyba jeden z najbardziej pożytecznych jego elementów. Widać, że autorzy dokonali bardzo dokładnego rozeznania w istniejącej literaturze na temat bezpieczeństwa ISE i bezpieczeństwa teleinformatycznej IK w ogóle. Zestawienie materiałów, które odnoszą się w całości lub w części do bezpieczeństwa ISE zawiera aż 54 pozycje. W zestawieniu, oprócz tytułu i odnośnika http do materiału online (w sytuacji kiedy takowy istnieje), jest też podstawowa ocena materiału poprzez określenie jego istotności w odniesieniu do tematu (określony trzema poziomami: niski, średni i wysoki), podana jest data publikacji i, w niektórych przypadkach, komentarze autorów.
Jeżeli kogoś interesują jeszcze bardziej precyzyjne odnośniki, to takowe zawiera załącznik C. W tabeli dla wszystkich zagrożeń wskazane są potencjalne narzędzia obronne wskazywane przez trzy systemy kompleksowo opisujące takie narzędzia, tj.: standard NIST, Enhancing Security Throughout the Supply Chain (IBM Center), Smart grid Information Assurance and Security Technology Assessment (sacramento State).

Wnioski z lektury

Raport ENISA nie jest materiałem, który załatwia za nas przygotowanie opracowania dotyczącego bezpieczeństwa ISE. Niemniej jednak dokument ten wydaje się być bardzo dobrym materiałem referencyjnym, w którym najważniejsze obszary są już w dużym stopniu usystematyzowane - np.: kwestie zasobów, zagrożeń czy narzędzi ochronnych, a reszta czyli szczegóły dotyczące tych obszarów są pokazane poprzez precyzyjny system referencji do obszernego katalogu materiałów źródłowych. Dlatego dla wszystkich, którzy mają wśród zadań kwestie bezpieczeństw ISE, dokument stworzony przez ekspertów ENISA będzie bardzo pomocny.

[1]http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012
[2] www.newshield.eu
[3]http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/terrorism-and-other-risks/index_en.htm
[4] http://www.crisalis-project.eu/
[5]http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5452993
[6]http://www.navigantresearch.com/wp-assets/uploads/2011/11/UCS-11-Pike-Research.pdf

KAŻDY MOŻE BYĆ WIELKI

Michał Rosiak

specjalista
ds. bezpieczeństwa
teleinformatycznego
Orange Polska

Artur Barankiewicz

kierownik Wydziału Analiz
i Strategii Bezpieczeństwa
Orange Polska

Wylatujące w powietrze stacje gazowe, elektryczność nie docierająca do punktów docelowych, a w efekcie gasnące oświetlenie, milknąca klimatyzacja, wyłączone światła na skrzyżowaniach dużych miast. Kolejny krok to już tylko apokaliptyczna anarchia na ulicach. Nie przypadkiem pierwsze skojarzenie to hollywoodzki film. Gorzej, że mówimy o czymś, co może – choć niekoniecznie w tak spektakularnej skali – zdarzyć się naprawdę.

Zgodnie z definicją, zawartą w art. 3 pkt. 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, infrastruktura krytyczna to: 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.
W jej skład wchodzą systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Pojęcie Teleinformatycznej Infrastruktury Krytycznej jest zatem bez wątpienia bardzo pojemne, a – co więcej – w dzisiejszych czasach, gdy światy teleinformatyczny i „analogowy" przenikają się w każdej płaszczyźnie, infrastruktura krytyczna i dbałość o jej bezpieczeństwo w bardzo wielu miejscach łączą się z kompetencjami dostawców usług internetowych (Internet Service Providers, ISP).

Reakcja musi być błyskawiczna

Co więcej, duży operator telekomunikacyjny sam jest elementem infrastruktury krytycznej, więc przede wszystkim trzeba zacząć od własnego podwórka. Pamiętajmy, że skuteczny atak cyber-terrorystyczny nie oznaczałby tylko „wyłączenia" internetu. To zdecydowanie krótkowzroczne myślenie, bowiem zamilkłyby też telefony, usługi oparte na telemetrii (również te świadczone dla innych elementów infrastruktury krytycznej). Im bardziej przerwa by się przedłużała, tym większe pojawiałoby się zamieszanie. Jeśli – co gorsza – towarzyszyłyby jej inne, bardziej spektakularne cyber-ataki, ostatecznie mogłoby się to przełożyć na panikę wśród milionów użytkowników. Dlatego tak, jak małego dziecka nawet na chwilę nie pozostawiamy bez opieki, niezbędne jest monitorowanie w trybie 24/7 przynajmniej kluczowych systemów teleinformatycznych pod kątem odpowiednio zdefiniowanych anomalii. Wbrew pozorom ta analogia nie jest naciągana – i jedno i drugie zostawione bez ochrony staje się praktycznie bezbronne, a potencjalne konsekwencje mogą być bardzo duże.

Odpowiednio przygotowane Centrum Operacji Bezpieczeństwa (Security Operations Center, SOC) to przede wszystkim doświadczeni ludzie, ale także wsparcie odpowiednich technologii oraz dopracowanych procedur operacyjnych. Bez technologii nie zawsze da się dojrzeć, że w sieci dzieje się coś złego, bądź też zamiast ostrzeżeń o faktycznych zagrożeniach, systemy będą generować fałszywe alarmy, zajmujące czas analitykom. Za przykład przydatności procedur może natomiast posłużyć szeroko opisywany w mediach poświęconych bezpieczeństwu IT przypadek amerykańskiego giganta detalicznego Target, skąd przestępcy wykradli dane 110 milionów klientów. Zainstalowane tam systemy bezpieczeństwa poinformowały o podejrzanej aplikacji niemal natychmiast po tym, gdy znalazła się w systemach, jednak alarmy zostały... zignorowane przez „specjalistów" od bezpieczeństwa. Odpowiednio przygotowane procedury nie dałyby im takiej dowolności w interpretacji, a wtedy faktycznego ataku udałoby się uniknąć.

Szeryf Chudy to za mało

A może jeśli nie da się subtelnie, to użyć brutalnej siły? Nie w rozumieniu hakerskim, ale jak najbardziej dosłownym – jeśli nie da się otworzyć zamka, to czemu go nie wyłamać? Jeśli nie da się włamać do serwerów, to zniszczmy serwery! Teoria, podobnie jak potencjalny wektor ataku, jak najbardziej słuszna. I tutaj tkwi – a przynajmniej tkwić powinno – jedno z głównych podobieństw między fizycznymi lokalizacjami różnych elementów infrastruktury krytycznej. Można by pół żartem powiedzieć, że gdyby nie infrastruktura krytyczna, to Specjalistyczne Uzbrojone Formacje Ochronne nie miałyby co robić, ale jak w każdym żarcie i tu jest ziarenko prawdy. Co nie zmienia faktu, że w przypadku zdarzeń losowych, czy klęsk żywiołowych nie pomoże nawet czołg. Dlatego budowa dużego Centrum Przetwarzania Danych to wyzwanie na wielu polach – również odporności na ekstremalne warunki atmosferyczne. Mimo to dla bezpieczeństwa przydałoby się zdublować kluczowe systemy – najlepiej w innej części kraju – i zapewnić odpowiednie procedury przełączania. Pamiętajmy też o opracowaniu i stosowaniu procedury backupu. Takie szczęście, jakie w 1999 roku mieli producenci Toy Story 2, zdarza się raz na sto lat. Wtedy ktoś niefortunnie wyczyścił dysk z produkcyjną kopią filmu, a system backupowy jak się okazało... przestał działać miesiąc wcześniej. Tam sytuację ocaliła jedna z pracownic, która

nielegalnie wyniosła kopię dla swojego syna, co w naszym przypadku jest po wielekroć niemożliwe: dziecko nie zainteresuje się raczej danymi z systemów ISP, czy przesyłu gazu, a wewnętrzne polityki bezpieczeństwa nie pozwolą zgrać istotnych danych na nośniki zewnętrzne. Nie wspominając już o tym, że byłoby tego znacznie więcej, niż w przypadku filmu o Szeryfie Chudym i jego kumplu...

Interes jest tylko wspólny

To właśnie dostawcy internetu *per se* stanowią pierwszą linię obrony Infrastruktury Krytycznej, jako jednostki generujące najwięcej ruchu sieciowego. Internet Service Provider, chroniąc przed atakami najpierw swoich Klientów i w następnym kroku własną infrastrukturę, może już na tym etapie „odsiać" dużą część złośliwego ruchu, choćby wycinając ruch zidentyfikowany jako związany z atakiem na własnych urządzeniach sieciowych, w momencie „wejścia" do krajowej sieci. O ile jednak takie rozwiązanie może pomóc, gdy cel ataku znajduje się w sieci operatora, co w przypadku, gdy dostęp do internetu dostarcza mu konkurencja? W tej dziedzinie akurat nie powinny istnieć granice, wynikające z codziennej konkurencji biznesowej – w przypadku udanego ataku na infrastrukturę krytyczną nie będzie podziału na abonentów sieci komórkowych, czy stacjonarnych. ISP, przede wszystkim w sytuacji, gdy mówimy o dużym dostawcy, ma tę przewagę, że uzyskane przezeń dane, dotyczące potencjalnych anomalii, są dzięki wielkości i rozpiętości jego infrastruktury bardziej reprezentatywne, niż w przypadku mniejszej próbki. Przy odpowiednio przygotowanych i dopracowanych zawczasu kanałach komunikacji „czerwona flaga", która podniesie się w SOC u monitorującego swoją sieć w trybie ciągłym Operatora może dać potencjalnej ofierze bezcenny czas na przygotowanie się do ataku (vide opisywany wcześniej casus firmy Target).

Powyższe, w ewidentny sposób udowodniły ćwiczenia CyberEXE, przeprowadzane przez Fundację Bezpieczna Cyberprzestrzeń. Pokazały one zarówno to, jak efektywna potrafi być współpraca między teoretycznie kompletnie nie związanymi ze sobą jednostkami, ale także potęgę informacji, których może dostarczyć Internet Service Provider oraz wymagające szybkiej poprawy niedociągnięcia na gruncie proceduralnym.

Pomóżmy informacji znaleźć adresata

„Informacja to potęga. Ale od Ciebie zależy, czy pozwolisz, by uczyniła Cię wielkim, czy zmarginalizowała" – ten cytat, przypisywany anonimowemu autorowi, znakomicie oddaje specyfikę dzisiejszego, wściekle szybko biegnącego świata. Dostawcy usług internetowych gromadzą dużo informacji i tylko do nich zależy jak i kiedy je przeanalizują, jakie wnioski z nich wyciągną, a także jak szybko i z kim się nimi podzielą. Szeroka współpraca z jednostkami ds. bezpieczeństwa IT z całego świata, pozwala na uzyskanie danych z innych części globu i może pomóc w efektywnym, proaktywnym przeciwdziałaniu atakom. To nie są dane, które trzyma się tylko dla siebie, ewentualnie dla najbliższych przyjaciół. Gdy chodzi o infrastrukturę krytyczną, to – jakkolwiek górnolotnie by to nie zabrzmiało – nie chodzi o firmy, biznes i zyski, tylko o Polskę i Polaków, a tutaj każdy, kto ma informacje, może – i bez wątpienia powinien – chcieć, by uczyniła go wielkim.

GŁÓWNE ZAGROŻENIA ŚRODOWISKA PRZEMYSŁOWYCH SYSTEMÓW STEROWANIA

Jacek Walaszczyk
EY Business Advisory

Środowisko przemysłowych systemów sterowania w ostatnich latach znacznie się zmieniło, postęp technologiczny przyniósł nowe funkcjonalności, a wraz z nimi nowe i zupełnie wcześniej nieznane zagrożenia.

Na przestrzeni kliku dekad komputeryzacja całkowicie zmieniła organizację pracy. Oczywiste więc było, że komputeryzacja zmieni również i przemysł. Od 1975 roku, gdy na rynku pojawił się pierwszy system DCS (ang. Distributed Control System) przemysłowe systemy sterowania zaczęły stopniowo wypierać sterowanie oparte na przekaźnikach. W rezultacie obecne systemy typu DCS są standardem w sterowaniu procesami ciągłymi w elektrowniach, rafineriach, zakładach chemicznych, kopalniach, przesyle gazu i ropy itp. Środowisko przemysłowych systemów sterowania było przez długi czas środowiskiem hermetycznym, tzn. stosowane były wyłącznie dedykowane, specjalistyczne rozwiązania, charakterystyczne wyłącznie dla środowiska automatyki przemysłowej - OT (ang. Operational Technology). Sieci przemysłowe były fizycznie odseparowane od sieci biurowych, protokoły komunikacyjne takie jak modbus, profibus, devicenet itp. były protokołami dedykowanymi dla przemysłu, sterowniki i kontrolery oparte były o dedykowane systemy operacyjne czasu rzeczywistego, a algorytmy sterowania kodowane w wyspecjalizowanych, dedykowanych językach programowania. XXI wiek przyniósł wiele zmian w hermetycznym dotąd środowisku OT. Systemy IT obecne w przemyśle dotąd jedynie w warstwie biznesowej (systemy ERP - ang. Enterprise Resource Planning, poczta elektroniczna, intranet) zaczęły przenikać do warstwy automatyki przemysłowej OT. Biznes zauważył dużą wartość danych z warstwy OT. Coraz częściej zaczął wykorzystywać dane pochodzące bezpośrednio z procesu technologicznego do prognozowania i planowania produkcji, kontrolowania wskaźników wydajności, jakości i dostępności. Odseparowane dotąd sieci IT i OT zaczęły się łączyć. Pomiędzy warstwą systemów klasy ERP a systemów SCADA (ang. Supervisory Control and Data Aquisition) nadzorujących proces sterowania, powstały systemy optymalizacji produkcji klasy MES (ang. Manufacturing Execution System) czy optymalizacji pętli sterowania klasy APC (ang. Advanced Process Control). Sieć systemów sterowania coraz częściej opiera się o sieć Ethernet i protokoły TCP/IP. Panele operatorskie HMI (ang. Human-Machine Interface) coraz powszechniej posiadające funkcję sterowania, nierzadko oparte są o system operacyjny Windows. Sterowniki PLC (ang. Programmable Logic Controller), systemy SCADA coraz częściej umożliwiają kodowanie algorytmów sterowania w znanych z IT językach, np. Basic, Pascal, C. Coraz częściej dane pomiarowe z urządzeń polowych przesyłane są bezprzewodowo. Stosowane są rozwiązania oparte o wirtualizację serwerów. Technologie bazujące na infrastrukturze telefonii komórkowej coraz częściej znajdują zastosowanie w przemysłowych systemach wymiany danych. Z aplikacjami typu SCADA współpracować mogą moduły, których zadaniem jest powiadamianie o zaistniałych zdarzeniach za pomocą wiadomości tekstowych lub poczty elektronicznej. Oprogramowanie klienta żądające alertów

może pracować na stacjach sieciowych i odwoływać się do usług świadczonych przez serwer. Komunikat jest wysyłany w postaci standardowej poczty elektronicznej poprzez Internet i protokół SMTP. Oprócz tego dane mogą docierać do użytkownika z wykorzystaniem poczty elektronicznej, za pomocą usług pocztowych oferowanych przez operatorów sieci komórkowych. Istnieje możliwość informowania użytkownika o zdarzeniach w procesie dzięki wiadomościom SMS. Niektóre systemy umożliwiają stworzenie WebSerwerów – wizualizacji procesu technologicznego, którą możemy podglądać przez przeglądarkę internetową. OT przyjmuje wiele ze środowiska IT – również zagrożenia, które wcześniej były obce dla przemysłowych systemów sterowania.

Zagrożenia technologiczne

W czasach, kiedy systemy OT posiadały wyspecjalizowane i specyficzne dla tego środowiska rozwiązania, zagrożenia dla ich funkcjonowania stanowiły przypadkowe błędy w produkcji czy związane z tym użytkowanie systemów teleinformatycznych. Celowy sabotaż musiał sprowadzać się do fizycznej ingerencji na terenie zakładu. Ochrona obiektów przemysłowych ograniczała się więc wyłącznie do ochrony fizycznej, zabezpieczenia systemów sterowania w inny sposób nawet nie rozważano. Dzisiaj możliwe jest przejęcie kontroli nad procesem technologicznym bez fizycznej obecności przy instalacji. Co więcej sabotażysta może być oddalony o tysiące kilometrów, wyposażony w komputer i dostęp do Internetu. Fizyczna ingerencja w instalacje z substancjami łatwopalnymi budzi strach i poczucie zagrożenia. Zdalny sabotaż okazuje się dużo bardziej niebezpieczny. Dużą rolę odgrywa bowiem psychologia, poczucie bezkarności i bezpieczeństwa, czy 'zdobyte trofeum', którym jest kolejny złamany system. Brak namacalnego zagrożenia i konsekwencji działania towarzyszące cyberprzestępcom jest bardzo poważnym zagrożeniem dla infrastruktury przemysłowej.

Coraz powszechniejsza inteligencja i autonomiczność urządzeń niesie ze sobą wiele nowych funkcjonalności oraz korzyści, w tym również ekonomicznych. Powstają bezobsługowe stacje, odwierty - instalacje stanowiące łatwy cel. Niestety często ochronę tego typu obiektów ogranicza się do zabezpieczeń technicznych (telewizja przemysłowa, bariery ultradźwiękowe, podczerwieni itp.). Uszkodzenie fizyczne instalacji czy fizyczne złamanie zabezpieczeń dużo łatwiej zidentyfikować niż zagrożenie, którego bezpośrednio nie widać, które zostanie wykryte dopiero po skutkach jakie przyniosło lub gdy jest jego świadomość i zostaną zastosowane odpowiednie środki ochrony. „Niewidoczne" zagrożenie rozumiane jest jako złośliwe oprogramowanie, wirus czy skrzętnie ukryty wycinek kodu programu sterującego procesem technologicznym, czekające na zainicjowane określonym zdarzeniem. Instalacja może pracować bezawaryjnie klika lat czekając na odpowiednią sytuację inicjującą ukryty algorytm, którego konsekwencje mogą być katastrofalne.

Wspomniane wcześniej wykorzystanie technologii bezprzewodowej do przesyłania danych procesowych do systemów sterowania daje spore korzyści ekonomiczne. Opomiarowanie jednego bloku energetycznego może wiązać się z dziesiątkami kilometrów przewodów. Oczywiste jest więc, że znaczne ograniczenie ilości drogiego medium przynosi spore oszczędności, nie należy jednak zapominać o bezpieczeństwie przesyłu tak istotnych danych jak dane procesowe. Sterowanie opiera się o informacjach z procesu odczytanych przez urządzenia polowe (czujniki temperatury, ciśnienia, przepływu, poziomu itp.). Coraz bardziej popularny staję się protokół Wireless HART, który służy do diagnostyki oraz zmiany ustawień urządzeń polowych bezprzewodowo. Przechwycenie transmisji i zmiana ustawień (np. zakresu czujnika ciśnienia) może stanowić wielkie zagrożenie dla procesu.

Odpowiednie zabezpieczenie medium, jakim jest fala radiowa, stanowi niemałe wyzwanie, które stanowi również odpowiednio zabezpieczona sieć korporacyjna połączona z siecią OT. Bezpieczeństwu nie sprzyja fakt, że sieć Ethernet staje się coraz bardziej popularna w środowisku przemysłowych systemów sterowania. Przy braku prawidłowej segmentacji sieci, wykorzystując narzędzia do skanowania w łatwy sposób można uzyskać informacje o adresach modułów Ethernetowych sterowników. Znając adres i posiadając odpowiednie narzędzie programowe można dostać się do kodu programu sterownika i zmienić czy zatrzymać proces. Popularyzacja standardu Ethernet ułatwiła dostęp do systemów sterowania. Jednak nie oznacza to braku zagrożenia, gdy komunikacja odbywa się po łączach szeregowych. W tym miejscu należy wyjaśnić, co kryje się pod pojęciem komunikacja szeregowa. Większość wykorzystywanych dziś standardów komunikacji, w tym wspomniany Ethernet, jest oparta na komunikacji szeregowej. W środowisku OT komunikacja szeregowa oznacza jednak asynchroniczną komunikację szeregową o niskiej przepustowości opartej o standardy EIA/TIA-232, EIA/TIA-422 czy EIA/TIA-485. Powszechny jest pogląd, że komunikacja szeregowa jest bezpieczna, co niestety nie jest prawdą. Wspomniane standardy komunikacji szeregowej są mniej popularne niż Ethernet, co zmniejsza ryzyko ataku, lecz go nie eliminuje. Przykładem może być informacja z 21 sierpnia 2012 roku podana przez NIST (National Institute of Standards and Technology) o podatnościach Korenix JetPort 5600 oraz ORing Industrial – serwerów portów szeregowych stosowanych w przemyśle. Firmware tych urządzeń miały zaszyte hasło „password" dla konta root, co pozwalało atakującemu uzyskanie dostępu administracyjnego za pośrednictwem sesji SSH.

Luki w zabezpieczeniach przytrafiają się także dostawcom rozwiązań OT. Pomimo sporej konkurencji na rynku, rosnącego znaczenia postrzegania marki i konsekwencji pojawiających się informacji o błędach producentów, nierzadko pojawiają się publikacje opisujące podatności sprzętu i systemów OT. Przykładem może być informacja podana przez ICS-CERT z 18 marca bieżącego roku o błędach w firmware switchy RuggedCom firmy Siemens dedykowanych dla środowiska OT. Wysyłając odpowiednie pakiety można zdalnie przeprowadzić atak blokujący urządzenie, bez konieczności uwierzytelniania. Przykładów podatności systemów i urządzeń OT jest sporo a każdy miesiąc przynosi informacje o nowo wykrytych podatnościach i lukach w rozwiązaniach dedykowanych dla środowiska OT. Dostawcy rozwiązań OT często świadczą zdalne usługi serwisowe, wdzwaniając się do modemów dial-up lub coraz częściej korzystając z sługi VPN, mają możliwość przejęcia kontroli nad urządzeniem RTU, sterownikiem PLC czy systemem SCADA. Atak może być przeprowadzony na komputery firmy, które współpracują z celem ataku i mają do niego dostęp poprzez chociażby wspomnianą usługę VPN.

Organizacja

Osobną grupę zagrożeń stanowią te związane z zarządzaniem środowiskiem OT. Poczucie bezpieczeństwa oparte na braku świadomości zagrożeń, brak odpowiedniego podejścia, metodyk do takich kwestii jak aktualizacje oprogramowania czy systemów operacyjnych na serwerach systemów sterowania bez wcześniejszego przetestowania ich wpływu na systemy OT czy brak odpowiednio wykwalifikowanej kadry może skutkować większym prawdopodobieństwem ryzyka awarii systemów sterowania niż w przypadku cyberataków. Usprawnienie zarządzania środowiskiem OT jest pierwszym krokiem, jakie powinny wykonać przedsiębiorstwa w celu zwiększenia bezpieczeństwa procesu.

Bezpieczeństwo

Zagadnienie bezpieczeństwa środowiska OT nie jest więc łatwe, mając na uwadze fakt, że zagrożenia systemów OT dotykają różnych obszarów. Proponuje się rozważyć bezpieczeństwo OT w trzech podstawowych warstwach: technologicznej, organizacyjnej i procesowej. W warstwie technologicznej znajduje się zabezpieczenie sprzętu począwszy od urządzań pomiarowych, przez sterowniki PLC, po serwery i stacje robocze systemów SCADA czy DCS. W warstwie tej znajduje się także bezpieczeństwo sieci tj. urządzeń sieciowych oraz protokołów komunikacyjnych. Warstwa organizacyjna dotyczy odpowiedniej struktury organizacyjnej, podziału ról i obowiązków, budowaniu kompetencji i świadomości. Warstwa procesowa to identyfikacja procesów oraz odpowiednie standardy, procedury i polityki opisujące zasady działania środowiska OT. Każda z trzech warstw musi być rozwinięta na odpowiednim poziomie by skutecznie zabezpieczyć infrastrukturę przemysłową.

Systemy sterowania nierzadko odpowiadają za prawidłowe funkcjonowanie najbardziej wrażliwej infrastruktury (w tym tzw. Infrastruktury Krytycznej), należy więc przyłożyć szczególną uwagę do zmniejszania ryzyka utraty kontroli nad środowiskiem OT.

PRYWATNY KLASTER WYSOKIEJ DOSTĘPNOŚCI

przy użyciu systemów Linux i Pacemaker

dr inż. Maciej Rostański

Często, gdy dochodzi do dyskusji na tematy związane z bezpieczeństwem systemów komputerowych, na pierwszym planie pojawiają się kwestie związane z poufnością oraz integralnością danych i systemów. Na dalszym planie dopiero pojawia się dostępność, która jednak stanowi nie mniej ważny element triady podstawowych atrybutów. Praktycznie każdy administrator przyzna, że przerwy w działaniu usług sieciowych organizacji są bardzo dotkliwe. Nawet, jeśli bezpośrednie skutki biznesowe niekoniecznie muszą być dużej skali, może się często okazać, iż zatrzymanie usług, do których pewności i trwałości użytkownicy są przyzwyczajeni, powoduje pośrednio duże straty. Prowadzi to do rozwiązań, w których podstawowe usługi sieciowe (takie jak e-mail czy zasoby www) są przedmiotem outsourcingu, migracji do środowisk w chmurze czy wirtualizacji w zewnętrznym data center.

Co jednak w przypadku, gdy aplikacja jest niestandardowa, gdy musi być użytkowana w lokalnym intranecie, gdy projekt zakłada minimalne koszta wejściowe i operacyjne? Jeśli natywny system operacyjny owej usługi należy do rodziny Linux, można taką aplikację uruchomić w klastrze wysokiej dostępności za pomocą oprogramowania Pacemaker.

Wysoka dostępność - odrobina teorii

Co do zasady, systemy HA (High Availability, wysokiej dostępności) oraz FT (Fault Tolerance, odporne na awarie) projektuje się według dwóch różnych od siebie wymagań. W przypadku wysokiej dostępności, chodzi o **zminimalizowanie czasu, w którym usługa jest niedostępna**. W przypadku odporności na awarie – absolutnym brakiem przestoju w ogóle, niezależnie od tego, jaki element systemu przestanie działać. Zasada w systemach HA jest prosta i zgodna z definicją dostępności (A), zależnej od średniego czasu pomiędzy awariami oraz średniego czasu naprawy (patrz ramka). **Rozwiązania projektowane z myślą o HA mają na celu jak największą dostępność, czyli jak najdłuższy czas nieprzerwanego działania**. Rozwiązania takie mogą zawierać wiele uzupełniających się elementów – dyski typu hot-swap, podwójne zasilanie, czy też pamięć wyższej klasy z automatyczną korekcją błędów - to przykłady zadbania o HA już na poziomie komponentów samych jednostek serwerowych. Można powiedzieć, że termin „wysoka dostępność" oznacza obecnie ogół metod, technik i rozwiązań pozwalających na osiągnięcie ustalonego poziomu dostępności w zakontraktowanym czasie. Podstawową zasadą jest tutaj **nadmiarowość (redundancja) elementów, zarówno fizycznych jak i logicznych**.

O ile nadmiarowość elementów fizycznych zależy tylko od budżetu projektu, zadbanie o nadmiarowość składników logicznych, takich jak aplikacja CRM czy też serwer plików, nie jest już zadaniem tak prostym. Są to bądź co bądź wyjątkowe elementy IT, specjalnie skonfigurowane, a uruchomienie ich ponownie (lub równolegle) w innym miejscu wymaga „przeniesienia" często również innych konfiguracji, jak chociażby adresu IP.

Rozwiązania HA w sieci przedsiębiorstwa średniego rozmiaru obecnie opierają się na dwóch różnych pomysłach:
a) Wykorzystaniu **wirtualizacji** (a konkretniej, mechanizmów wbudowanych w hyperwizory, pozwalających na szybkie odtworzenie maszyny wirtualnej, nawet w innej lokalizacji).
b) Wykorzystaniu **klastrowania** (ściślej: skonfigurowaniu pewnej liczby systemów w klaster, aby mogły razem decydować o uruchamianiu usług). Na tej idei koncentruje się niniejszy artykuł.

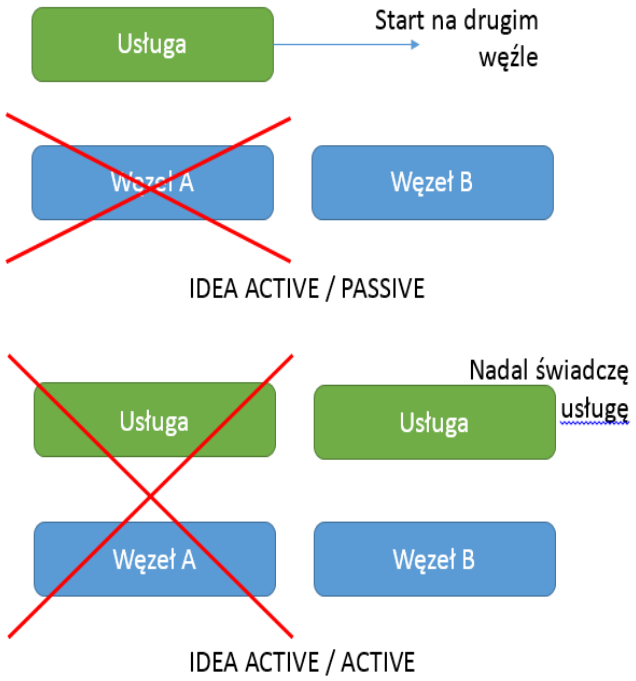
***Dostępność (Availability)** można określić za pomocą wzoru:*

$$A = \frac{MTBF}{MTBF + MTTR}$$

gdzie MTBF to średni czas pomiędzy awariami, a MTTR to średni czas naprawy.
Wynika z tego, że najlepiej mieć jak najkrótszy czas naprawy. A awarie? Zdarzać się przecież będą i tak.
Można również zdefiniować dostępność jako procentowy stosunek czasu działania do czasu mierzonego. Sławne „pięć dziewiątek" oznacza 99,999% dostępności.

Koncepcję działania klastra HA przedstawiono na rys. 1. Usługę można skonfigurować do działania na więcej niż jednej maszynie, co pozwoli na uruchomienie natychmiast w nowej lokalizacji w przypadku awarii starej (koncepcja *Active/Passive*), lub też, jeśli tylko usługa na to pozwala, uruchamia się ją naraz w wielu lokalizacjach, aby awaria jednej z nich nie powodowała przerwania usługi (koncepcja *Active/Active*).
Istnieją przypadki szczególne, z których najważniejsze to:

- N+1 (klaster wielu usług z jednym węzłem zapasowym dla jakiejkolwiek usługi),
- N+M (wiele usług uruchomionych naraz na wielu węzłach, dodatkowo pewna ilość węzłów przygotowanych na awaryjne przeniesienie (ang. *failover*).



Rysunek 1. Koncepcje rozwiązań HA

Z czego składa się klaster HA?

Podstawowym składnikiem klastra są maszyny wchodzące w jego skład (zwane od tego momentu **węzłami**, ang. *nodes*) oraz oprogramowanie, dzięki któremu komunikują się nawzajem, czyli tzw. **menedżer klastra**. Menedżer klastra musi być uruchomiony na każdym węźle, a dodatkowo jeden z węzłów zostaje wybrany głównym, aby móc podejmować decyzje w imieniu całego klastra. Komunikacja między węzłami trwa nieprzerwanie – w razie przerwania transmisji z którymś z węzłów, reszta klastra przyjmuje, że uległ on awarii. Analogicznie sytuacja odwraca się w przypadku przywrócenia nadawania przez uprzednio utracony węzeł. Gdy wszystkie węzły mają podobne możliwości sprzętowe i wydajnościowe, klaster jest **symetryczny**; gdy węzły mają różne zasoby sprzętowe i programowe, klaster nazywa się **asymetrycznym**.

Z węzłami oraz ewentualnymi brakami w komunikacji wiążą się jeszcze dwa pojęcia: **kworum** klastra (ang. *quorum*) oraz mechanizmy **odcięcia** (ang. *fencing*). W przypadku kłopotów z komunikacją może zaistnieć sytuacja, w której nie tylko jeden, ale i więcej węzłów zostanie od siebie odseparowanych; tylko jedna grupa, posiadająca kworum, ma prawo wówczas podejmować decyzje dotyczące działania usług. Z reguły kworum jest obliczane na podstawie zwykłej większości głosów („demokracja"), ale jest więcej algorytmów wyznaczania kworum, co ma znaczenie zwłaszcza dla klastrów asymetrycznych („duży może więcej"). W przypadku, gdy grupa posiadająca kworum uzna, iż jakiś węzeł należy wyłączyć lub uruchomić ponownie z pewnych względów (może to być na przykład węzeł, który blokuje dostęp do współdzielonych zasobów dyskowych), używa dostępnych mechanizmów odcięcia, których przykłady opisano w dalszej części tekstu
.
Na rys. 2 pokazano wynik polecenia monitorującego klaster skonfigurowany przy użyciu trzech węzłów (Alpha, Bravo, Charlie). Jednocześnie widać, iż grupa posiada kworum, a także, że węzłem głównym (DC, ang. *Designated Co-ordinator*) jest obecnie węzeł Charlie.

```
[root@Charlie ~]# pcs status
Cluster name: ha_cluster
Last updated: Mon Feb  3 12:55:04 2014
Last change: Mon Feb  3 12:31:30 2014 via cibadmin on Charlie
Stack: cman
Current DC: Charlie - partition with quorum
Version: 1.1.10-14.el6_5.2-368c726
3 Nodes configured
0 Resources configured


Online: [ Alpha Bravo Charlie ]
```

Rysunek 2. Informacje o stanie klastra.

Najważniejszym składnikiem jest jednak nie tyle podstawa fizyczna, czyli węzły wraz z menedżerem klastra, ale oprogramowanie, które przy pomocy menedżera klastra zarządza węzłami, samo natomiast ustala, jakie usługi oraz na jakim węźle mają być uruchomione. Jest to **menedżer zasobów** i od jego możliwości zależy, jak wiele rozwiązań będzie można zastosować w realizowanym klastrze HA.

Zasobów może być bardzo wiele, bo są to wszystkie logiczne składniki systemu – od zamontowanych zasobów dyskowych czy skonfigurowanych adresów IP, po aplikacje serwerowe czy monitorujące. Podstawowym zadaniem menedżera zasobów jest kontrola „stanu zdrowia" wszystkich usług mu podległych, ponowne uruchamianie, czy też podejmowanie decyzji o ewentualnej migracji do innych lokalizacji.

Oprogramowanie w środowisku Linux

Na wiodące rozwiązanie klastra HA w środowiskach open-source wyrasta **duet *corosync – pacemaker***. *Corosync* jest menedżerem klastra – umożliwia synchronizację węzłów, wspiera szyfrowanie komunikacji pomiędzy węzłami, nadmiarowość połączeń pomiędzy węzłami (tzw. pierścienie, ang. *rings*), dostarcza także mechanizmy określania kworum. Ale to *pacemaker* („rozrusznik", patrz ramka) jest tutaj kluczowym komponentem – menedżerem zasobów wspierającym wszystkie funkcje opisane wcześniej, a także wiele dodatkowych:

- Uruchamianie i zatrzymywanie usług / zasobów,
- Podejmowanie ww. decyzji na podstawie ustalonych zasad,
- Utrzymywanie historii i parametrów (np. licznik awarii),
- Ewentualna migracja zasobów na inne węzły,
- Uruchamianie lub zatrzymywanie dodatkowych instancji zasobów,
- Uwzględnianie wzajemnych związków pomiędzy zasobami (np. „nigdy razem"),
- Uruchamianie mechanizmów odcięcia (*fencing*).

Informatyczna gra słów

Poprzednikiem pakietu corosync w systemach Linux był heartbeat („bicie serca", czy też puls), nazwany tak od mechanizmu kontrolowania obecności węzłów poprzez krótkie rytmiczne komunikaty. Skoro węzły mają puls, to jakże nie nazwać pakietu uruchamiającego usługi inaczej niż pacemaker („rozrusznik")?

Pacemaker jest oprogramowaniem dostępnym w dystrybucjach całkowicie otwartych (Debian, CentOS), jak i używany w dystrybucjach biznesowych (SuSE Linux Enterprise Server, RedHat Enterprise Linux od 7.0). Konfiguracja jest możliwa zarówno w trybie powłoki, jak i w trybie graficznym, choć dostępność odpowiednich narzędzi graficznych zależy od systemu operacyjnego.

Zasoby pod kontrolą *Pacemakera*

Można wyróżnić kilka sposobów, za pomocą których Pacemaker kontroluje zasoby. Część zasobów jest zarządzana dzięki natywnym skryptom, rozwijanym od czasu projektu heartbeat (np. adres IP czy IPv6), część przy użyciu specjalnie przygotowanych agentów zgodnych ze specyfikacją OCF (ang. Open Clustering Framework). Jeśli aplikacja/usługa jest zgodna ze standardem LSB (ang. Linux Standards Base), czyli zwraca odpowiednie kody błędów, to menedżer nie będzie miał żadnego kłopotu z zarządzaniem tą usługą.

Dany zasób może być skonfigurowany jako klon, czyli usługa uruchomiona wielokrotnie na różnych węzłach, a także jako zasoby wielostanowe (master/slave), przydatne w przypadku gdy aplikacja wspiera „własnymi siłami" sytuację wielokrotnego jej uruchomienia i sama kontroluje komunikację pomiędzy swoimi instancjami (przykładem może być baza danych MySQL).

Specjalną kategorię stanowią mechanizmy do odcięcia (*fencing*). Pacemaker używa tutaj technologii STONITH (ang. *Shoot The Other Node In The Head*), który do działania potrzebuje interfejsów do wyłączenia danej maszyny – mogą one być oparte na urządzeniach rezerwujących (np. SCSI storage, FibreChannel), na urządzeniach dostarczających prąd typu wewnętrznego (np. HP iLO, IPMI, IBM Bladecenter, Cisco UCS) lub zewnętrznego (np. APC, WTI). Mogą też być oparte o inne metody (np. vSphere lub SNMP).

Proste studium przypadku

Na co w takim razie pozwala użycie Pacemakera? Jako prosty przykład posłuży intranetowa aplikacja WWW, będąca nakładką na bazę danych klientów. Wdrożenie obejmuje uruchomienie dwuwęzłowego klastra, a pliki aplikacji są umiejscowione na współdzielonym dysku sieciowym. Czego potrzebuje każdy z węzłów? Skonfigurowania serwera WWW oraz oprogramowania HA. Resztę przydziela menedżer zasobów, skonfigurowanych jak na rys. 3.

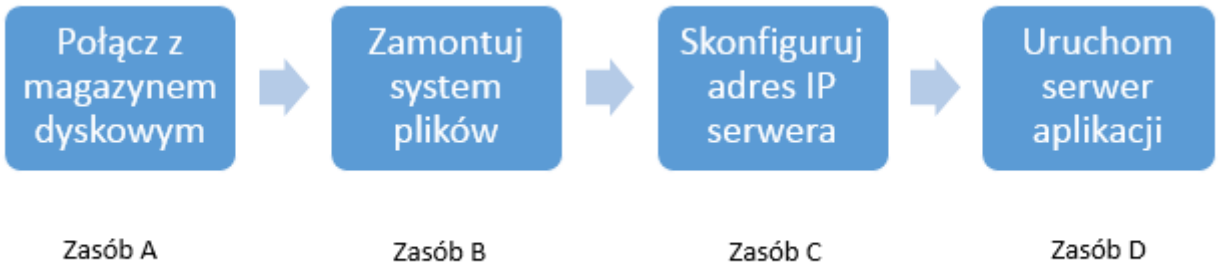
Menedżer zasobów można przy tym poinformować, aby używał:

- **strategii lokalizacji**, czyli preferował pewien węzeł (strategia „Opt-in") lub unikał danego węzła (strategia „Opt-out"),
- **strategii minimalizacji migracji**, czyli ważniejsze od wybrania węzła było pozostawienie zasobu w lokalizacji, w której już działa (tzw. stickiness),
- **strategii kolokacji lub antykolokacji**, czyli zasób aplikacji uruchomiony był na tym samym węźle co np. baza danych (lub na pewno na innym),
- **porządkowania**, co oznacza, że zasób może uzależnić swój start od działania innych zasobów.

Podsumowanie

Projektując rozwiązania bezpieczeństwa systemów informatycznych należy pamiętać o wymaganiach związanych z zapewnieniem dostępności do usług sieciowych. Często jednak podstawowym problemem jest konieczność kompromisów technicznych związanych z ograniczonym budżetem na wysokiej klasy rozwiązania. Oprogramowanie pacemaker jest sposobem na rozwiązanie bazujące na open-source, jednocześnie sprawdzone, zaadoptowane przez wiodące systemy linuksowe, w tym również klasy Enterprise, co pozwala na pewien poziom zaufania do tej technologii. Przy pomocy elastycznych mechanizmów zarządzania zasobami, można wprowadzić do swoich systemów elementy wysokiej dostępności (HA), ale także zrealizować strategię Disaster Recovery poprzez umożliwienie szybkiej migracji do nowej lokalizacji. Gama mechanizmów do wykorzystania jest na tyle szeroka, że pozwala na zaprojektowanie i wdrożenie bardzo zróżnicowanych scenariuszy realizacji wysokiej dostępności.

dr inż. Maciej Rostański - Informatyk - specjalista w zakresie niezawodności systemów komputerowych, wykładowca akademicki w Wyższej Szkole Biznesu w Dąbrowie Górniczej, instruktor Akademii Sieci Cisco, ekspert Narodowego Centrum Badań i Rozwoju.



Rysunek 3. Przykład konfiguracji i kolejności uruchamiania zasobów

Poszerzając zakres CIIP focusa wprowadzamy nową część Informatora poświęconą prezentacji projektów z zakresu bezpieczeństwa teleinformatycznego finansowanych ze środków Narodowego Centrum Badań i Rozwoju. Pierwszy artykuł poświęcony będzie projektowi pt. „Prototyp systemu perymetrycznej ochrony telekomunikacyjnej infrastruktury krytycznej" zrealizowanego przez Instytut Łączności – Państwowy Instytut Badawczy.

System ochrony sieci kablowych SPOT

Krzysztof Borzycki (Instytut Łączności),
Stanisław Dziubak (Instytut Łączności),
Paweł Gajewski(Instytut Łączności),
Michał Jabłoński (Asseco Poland SA).

System monitoringu sieci kablowych SPOT do scentralizowanego wykrywania uszkodzeń i ingerencji w telekomunikacyjnych sieciach kablowych został opracowany przez Instytut Łączności i Asseco Poland SA w latach 2010-2012, w ramach projektu rozwojowego NCBiR OR00012612. Elementy SPOT znajdują się w próbnej eksploatacji w sieci Orange Polska.

Telekomunikacyjna infrastruktura kablowa jest narażona na uszkodzenia w wyniku m.in.: robót ziemnych budowlanych i drogowych, wandalizmu, sabotażu i kradzieży kabli, degradacji kabli i osprzętu pod wpływem starzenia, korozji, wilgoci, uszkodzeń od warunków atmosferycznych, oblodzenia, powodzi, osuwisk, itp. Intensywność uszkodzeń najwyższa jest w sieciach ułożonych w ziemi. Spotyka się też nielegalne układanie przez operatorów alternatywnych swoich kabli w kanalizacji Orange Polska bez uzgodnień i opłat. Przeciwdziałanie kradzieżom, sabotażowi i nielegalnym pracom wymaga zamykania i monitorowania wszystkich studni kablowych.

Sieci zawierają też liczne obiekty bezobsługowe: szafy kablowe, szafy dostępowe z urządzeniami VDSL i TV kablowej czy stacje bazowe sieci komórkowych (BTS), narażone na działanie warunków atmosferycznych, wandalizm i kradzieże. Samych BTS jest w Polsce około 30 tysięcy. Operatorzy potrzebują narzędzi do monitoringu sieci kablowej i wspomagania jej utrzymania, by zagwarantować wskaźniki dostępności i szybkości usuwania uszkodzeń.

Monitoring kabli z parami przewodów miedzianych

Gros uszkodzeń linii kablowych powoduje nagłą przerwę lub zwarcie wszystkich par przewodów w kablu, co powoduje, że wystarcza monitorowanie jednej wolnej pary w celu wykrycia uszkodzenia. Głowice pomiarowe (GP) wykonują cyklicznie pomiary rezystancji pętli przewodów, a w razie potrzeby także pojemności między przewodami. Wyniki tych pomiarów są przesyłane do centrum nadzoru, gdzie następuje ich porównanie z wartościami wzorcowymi i dopuszczalnymi odchyłkami; na tej podstawie jest podejmowana decyzja o alarmie a następnie wyznaczana odległość do miejsca uszkodzenia. Zakresy pomiaru rezystancji (0-4095 Ω) i pojemności (0-1 μF) umożliwiają nadzorowanie linii z przewodami o średnicy 0,5-0,8 mm i długości do 15 km.

Charakterystyka techniczna systemu SPOT

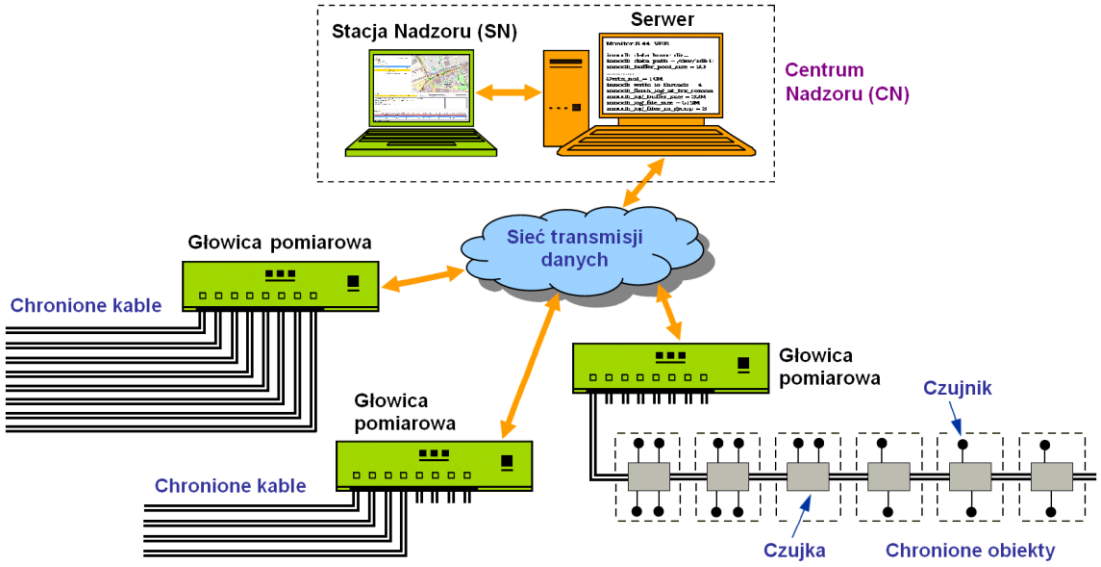
System SPOT, przedstawiony na rys. 1 umożliwia:

- monitorowanie ciągłości i parametrów (R, C) par przewodów miedzianych,
- lokalizację uszkodzeń kabli miedzianych,
- monitorowanie obiektów bezobsługowych za pomocą czujników,
- wprowadzanie i prezentację opisów obiektów i danych kontaktowych,
- sygnalizację uszkodzeń oraz prezentację elementów sieci i uszkodzeń na mapie,
- rejestrację i archiwizację zdarzeń w sieci,
- tworzenie raportów z danymi selekcjonowanymi według kryteriów użytkownika.

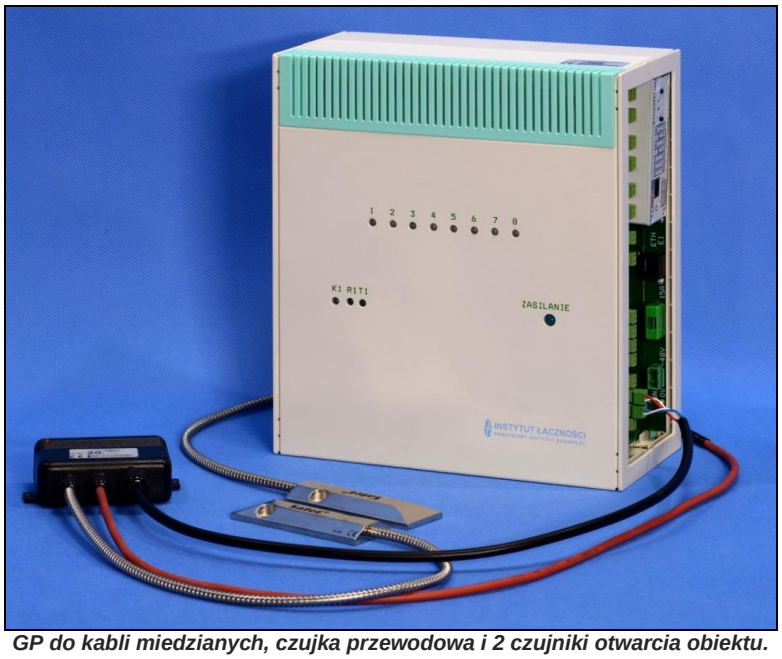
System nadzoruje obiekty bezobsługowe za pomocą czujek posiadających do kilku czujników różnych typów (otwarcia obiektu, temperatury, gazu, itp.) zdalnie zasilanych z GP napięciem stałym 62V. Głowica pomiarowa dla kabli miedzianych (rys. 2) ma 8 uniwersalnych wejść do obsługi czujek lub nadzoru kabli i 8 wejść tylko do nadzoru kabli. Każde z 8 wejść GP do obsługi czujek umożliwia monitorowanie kilkudziesięciu czujek wzdłuż linii o długości do 5-8 km. Dokładne dane systemu są ustalane indywidualnie dla każdej instalacji.

Centrum nadzoru systemu składa się z serwera i dołączonych do niego przez sieć Ethernet stacji nadzoru – komputerów PC z wyspecjalizowanym oprogramowaniem, używanym przez operatorów weryfikujących alarmy i przekazujących zlecenia napraw lub interwencji do firm serwisowych, agencji ochrony lub jednostek policji.

.



Konfiguracja systemu monitoringu SPOT



GP do kabli miedzianych, czujka przewodowa i 2 czujniki otwarcia obiektu.

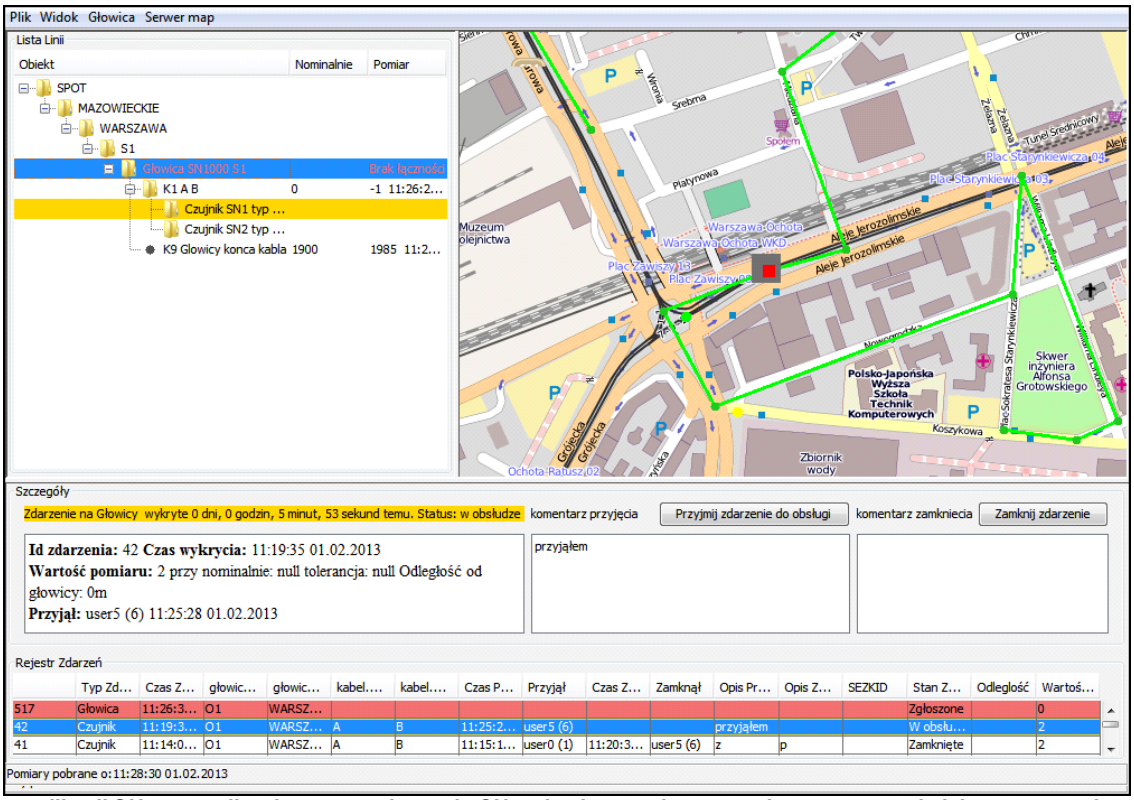
Serwer CN współpracuje z rozmieszczonymi w chronionej sieci głowicami pomiarowymi, które są z nim połączone za pośrednictwem sieci transmisji danych, wykorzystując protokół transmisji UDP lub TCP/IP. Umożliwia to scentralizowany nadzór sieci przy praktycznie dowolnej liczbie i lokalizacji GP.

Oprogramowanie Centrum Nadzoru

Oprogramowanie serwera Centrum Nadzoru i Stacji Nadzoru realizuje funkcje związane z:

- zbieraniem i obróbką danych pomiarowych z GP,
- wykrywaniem, sygnalizacją i lokalizacją uszkodzeń,
- instalacją, konfigurowaniem i nadzorem pracy własnych elementów sprzętowych,
- wprowadzaniem danych chronionych elementów sieci,
- utrzymywaniem bazy map cyfrowych,
- zarządzaniem użytkownikami o różnych poziomach uprawnień.

System generuje raporty ze zdarzeń filtrowanych według podanych przez użytkownika kryteriów: daty, typu, rejonu, rodzaju obiektu i innych. Oprogramowanie nadzoruje też pracę GP i ciągłość połączeń z nimi przez zewnętrzną sieć transmisji danych (rys. 3).



Ekran aplikacji SN z sygnalizacją utraty połączenia CN z głowicą pomiarową, pokazaną na mapie jako czerwony kwadrat.

Podsumowanie

System ochrony infrastruktury telekomunikacyjnej SPOT jest obecnie testowany w sieci Orange w dwóch miejscowościach w Polsce, służąc głównie do nadzoru studni kablowych. W przygotowaniu jest wersja do monitoringu sieci światłowodowych, wykorzystująca okresowe pomiary reflektometryczne (OTDR).

Powstaje raport:

Bezpieczeństwo infrastruktury krytycznej – wymiar teleinformatyczny

Joanna Świątkowska

ekspert ds. cyberbezpieczeństwa
Instytut Kościuszki

Ruszyły prace nad nowym raportem Instytutu Kościuszki poświęconym bezpieczeństwu infrastruktury krytycznej. Kluczowy element analizy stanowił będzie wymiar ochrony teleinformatycznej. Wydarzenia ostatnich lat, mające miejsce nie tylko w Gruzji czy Estonii, ale także ostatnio na Ukrainie i wielu innych miejscach, pokazują jak ważnym problemem z punktu widzenia stabilnego funkcjonowania państwa jest cyberbezpieczeństwo. Celem Raportu będzie przygotowanie rekomendacji zwiększających bezpieczeństwo Polski. Jednocześnie część dobrych praktyk może stanowić wsparcie dla budowania bezpieczeństwa także w innych krajach.

Systemy teleinformatyczne w coraz większym stopniu znajdują zastosowanie w najważniejszych obiektach, instalacjach, urządzeniach oraz usługach, zidentyfikowanych i wyznaczonych jako infrastruktura krytyczna państwa. Z uwagi na fundamentalną rolę tych systemów, zapewnianie prawidłowego ich funkcjonowania staje się newralgiczne z punktu widzenia bezpieczeństwa i zapewnienia żywotnych interesów państwa.

Ochrona infrastruktury krytycznej, także w wymiarze teleinformatycznym, znajduje się w centrum zainteresowania i prac podmiotów odpowiedzialnych za bezpieczeństwo Polski. W ostatnim czasie Rządowe Centrum Bezpieczeństwa przygotowało Narodowy Program Ochrony Infrastruktury Krytycznej, w którym cyberbezpieczeństwo stało się istotnym elementem ogólnych działań związanych z zapewnianiem ochrony infrastruktury krytycznej. Ponadto, Biuro Bezpieczeństwa Narodowego, na zlecenie Prezydenta RP, dokonało Strategicznego Przeglądu Bezpieczeństwa Narodowego, na podstawie którego powstała Biała Księga Bezpieczeństwa Narodowego RP. Również w tym dokumencie tematyka cyberbezpieczeństwa infrastruktury krytycznej została szeroko omówiona.

Także ze względu na „medialność" tematu, w doniesieniach prasowych i wypowiedziach publicznych bardzo często spotkać można odniesienia do cyberbezpieczeństwa infrastruktury krytycznej. Niestety materiały te cechuje częste nadużywanie lub niewłaściwie stosowanie omawianych terminów.

Z uwagi na rolę i wagę infrastruktury krytycznej w funkcjonowaniu obywateli, podmiotów komercyjnych i publicznych, jak również z uwagi na fakt, że jej bezpieczeństwo ma ścisły związek z całościowym bezpieczeństwem państwa, Instytut Kościuszki postanowił przygotować kompleksowy raport poświecony ochronie infrastruktury krytycznej. W sposób szczególny raport odnosił się będzie do zagadnień związanych z zapewnianiem bezpieczeństwa funkcjonowania systemów teleinformatycznych zastosowanych w infrastrukturze krytycznej.

Zarówno wspomniane wyżej NPOIK jak i Biała Księga wskazały kierunki i obszary, które z punktu widzenia zapewnienia bezpieczeństwa infrastruktury krytycznej powinny stać się elementem dalszych prac kluczowych interesariuszy. Poprzez swój raport i rekomendacje w nim zawarte, Instytut Kościuszki chce wesprzeć wszystkie podmioty zaangażowane w ten proces. Raport będzie ważnym głosem w debacie na temat tego kluczowego obszaru dla bezpieczeństwa kraju.

Raport składał się będzie z dwóch części. W pierwszej z nich, mającej charakter wprowadzający, przedstawione zostaną najważniejsze elementy związane z tematyką infrastruktury krytycznej. Celem będzie usystematyzowanie wiadomości i wskazanie prawidłowego rozumienia i stosowania najważniejszych terminów. Szczegółowej analizie poddane zostaną między innymi zagadnienia związane z procesem identyfikacji i wyznaczania infrastruktury krytycznej, rolą i kompetencjami organów zaangażowanych w jej ochronę, kluczowymi zagrożeniami i zadaniami odnoszącymi się do zapewniania bezpieczeństwa infrastruktury krytycznej. Ponadto rekomendacje dotyczyć będą prawnych aspektów związanych z ochroną infrastruktury krytycznej oraz zasad efektywnej współpracy prywatno - publicznej.

Druga część publikacji poświęcona zostanie stricte bezpieczeństwu systemów teleinformatycznych zastosowanych w infrastrukturze krytycznej. Otworzy ją analiza roli jaką odgrywają owe systemy teleinformatyczne, omówione zostaną zagadnienia związane z zagrożeniami i zapewnianiem bezpieczeństwa zarówno systemów informatycznych jak i systemów sterowania przemysłowego. W dalszej części zaprezentowana zostanie problematyka reagowania na incydenty teleinformatyczne w obszarze infrastruktury krytycznej i analiza programu studiów wyższych w zakresie ochrony systemów teleinformatycznych stosowanych w infrastrukturze krytycznej. Rozdział ten uzupełni spojrzenie na międzynarodowe inicjatywy związane z teleinformatycznym wymiarem ochrony infrastruktury krytycznej.

Zaproszenie Instytutu Kościuszki do wzięcia udziału w pracach nad przygotowaniem Raportu przyjęło Rządowe Centrum Bezpieczeństwa oraz Biuro Bezpieczeństwa Narodowego. Partnerem Głównym Raportu i współautorem jest firma EY. Ponadto poszczególne rozdziały Raportu przygotowane zostaną przez ekspertów z firmy MATIC, Politechniki Krakowskiej, Wojskowej Akademii Technicznej, Fundacji Bezpieczna Cyberprzestrzeń oraz Kancelarii Prawniczej - Wierciński Kwieciński Baehr.

Raport przygotowany zostanie w ramach projektu Instytutu Kościuszki pt. Cel: Cyberbezpieczeństwo.

W dniach 28-30 kwietnia europejskie państwa rozpoczęły ćwiczenia Cyber Europe 2014. Największe, europejskie ćwiczenia z zakresu ochrony cyberprzestrzeni. We wszystkich fazach udział weźmie ponad 600 uczestników.

Cyber Europe 2014

Redakcja

Z końcem kwietnia ponad 200 organizacji i ponad 400 ekspertów bezpieczeństwa teleinformatycznego z całej Europy przystąpiło do pierwszej, technicznej fazy ćwiczenia Cyber Europe 2014. Reprezentowali oni dwadzieścia dziewięć krajów: Państw Członkowskich Unii Europejskiej oraz państw zrzeszonych w Europejskim Stowarzyszeniu Wolnego Handlu.

Faza techniczna polegała na rozwiązywaniu incydentów, które zostały przygotowane przez Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA) i których podstawą opracowania były zdarzenia historyczne z ostatnich lat. Uczestnicy - przedstawiciele zarówno sektora publicznego jak i prywatnego, zespołów reagowania na incydenty komputerowe, ministerstw, instytucji badawczych, operatorów kluczowej infrastruktury energetycznej i telekomunikacyjnej, poproszeni zostali do zbadania i przeanalizowania kilku scenariuszy, które mogłyby w rzeczywistości zagrozić bezpieczeństwu zasobów teleinformatycznych.

- Incydenty Cyber Europe 2014 są bardzo realistyczne – komentuje prof. Udo Helmbrecht, dyrektor zarządzający ENISA – symulują niepokój i kryzys polityczny na poziomie europejskim oraz zakłócenia funkcjonowania usług dla milionów obywateli Europy. Cyber Europe 2014 to kamień milowy dla umocnienia współpracy przy sytuacjach kryzysowych w obszarze cyberprzestrzeni, zwiększenia gotowości i poprawienia zdolności reagowania na nie w całej Europie. – Zarówno polscy uczestnicy ćwiczeń jak i ich koledzy z zagranicy ocenili incydenty jako wymagające, ale też i ekscytujące – mówi Michał Grzybowski, moderator ćwiczeń – największą niedogodnością pozostawała Cyber Exercise Platform, nowatorska platforma, która zapewniała zarządzanie ćwiczeniem i niestety wymagała od uczestników wiele cierpliwości. Na szczęście polskie zespoły się nią wykazały, a co więcej udowodniły, że należą do ścisłej europejskiej czołówki i za to należą im się gratulacje.

Ćwiczenia Cyber Europe organizowane są co dwa lata przez Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency – ENISA) we współpracy z Państwami Członkowskimi Unii Europejskiej i członkami Europejskiego Stowarzyszenia Wolnego Handlu (EFTA). Do tej pory odbyły się dwie edycje ćwiczeń – w roku 2010 i 2012 (relację z Cyber Europe 2012 można przeczytać we wcześniejszych numerach CIIP focus). W porównaniu do poprzednich, tegoroczna edycja zaplanowana została na większą skalę, z udziałem większej ilości uczestników i cechuje się znacznie wyższym poziomem skomplikowania, zarówno samego przedsięwzięcia, które przewiduje rozegranie trzech faz (technicznej, operacyjnej i strategicznej) jak i samego scenariusza głównego.