Nr 2 - Wrzesień 2012

CIIP focus

RCB
Rządowe Centrum Bezpieczeństwa

informator o ochronie teleinformatycznej

CYBER-EXE POLSKA 2012

Pierwsze w Polsce ćwiczenia z zakresu ochrony przed cyberatakiem na infrastrukturę o strategicznym znaczeniu dla państwa – s.4

logo: Fundacja Bezpieczna Cyberprzestrzeń

W NUMERZE:

Drodzy Czytelnicy,

Zapraszamy do zapoznania się z drugim numerem informatora *„CIIP focus”.* Dziękujemy za duże zainteresowanie pierwszym numerem. Kilkaset pobrań informatora ze strony www było dla nas miłym zaskoczeniem, a jednocześnie potwierdzeniem naszych przypuszczeń, że tematyka, którą się zajęliśmy jest bardzo ważna i oczekiwana. Co prawda brakuje nam informacji od Państwa na temat tego co sądzicie o informatorze, ale próbujemy temu kłopotowi zaradzić i w tym numerze również zachęcamy do kontaktu, za zachętę wzmacniamy organizacją konkursu na najciekawszą opinię.

Bieżący numer w dużej części poświęcony jest pierwszym polskim ćwiczeniom z ochrony infrastruktury o strategicznym znaczeniu w cyberprzestrzeni. 19 września we Wrocławiu zaplanowane takie ćwiczenia w Polsce, a nasza redakcja jest mocno zaangażowana w przygotowania i przeprowadzenie tych ćwiczeń. W przygotowaniach do ćwiczeń mamy wsparcie Europejskiej Agencji Bezpieczeństwa Sieci i Informacji ENISA, stąd wywiad z pracownikami Agencji, którzy opowiadają między innymi jak ENISA wspiera państwa członkowskie w przygotowaniach do ćwiczeń takich jak nasze. Przez ostatnie kilka miesięcy poświęciliśmy, wraz kilkunastu innymi reprezentantami wielu polskich firm i instytucji, dużo czasu aby były to ćwiczenia udane. Mamy nadzieje, że tak będzie i w następnym numerze będziemy mogli się z Państwem podzielić wnioskami z ćwiczeń.

Tymczasem zachęcamy do zapoznania się z innymi tematami bieżącego numeru. Czeka na Państwa następny odcinek z „CERT Corner” a także specjalistyczne artykuły specjalistów od spraw ochrony infrastruktury krytycznej. Na koniec informacje o toczącym się projekcie naukowo-badawczym, którego celem jest budowa systemu „Bzura”, który jest pomysłem na kompleksowe podejście do zagadnienia bezpieczeństwa teleinformatycznego.

Życzymy miłej lektury!

Redakcja CIIP focus

KONKURS!

Zapraszamy do dzielenia się swoimi opiniami
i pomysłami dotyczącymi CIIP focus.
Autor najciekawszego listu nadesłanego do redakcji
zostanie nagrodzony
koszulką Cyber-EXE Polska 2012!
Konkurs trwa do 31 października 2012 r.
ciip-focus@rcb.gov.pl

NEWS

Washington Post ujawnia współpracę USA i Izraela przy produkcji złośliwego oprogramowania

Sprawa dotyczy dwóch słynnych wirusów – Stuxnet i Flame. Amerykańska gazeta twierdzi, że były one wspólną produkcją USA i Izraela, a celem było zmapowanie irańskich sieci komputerowych i ataki wymierzone w irański program nuklearny. Powiązania kodów obydwu wirusów zostały już udowodnione przez firmy zajmujące się analizą złośliwego oprogramowania.

http://bit.ly/QkM5AN

Techniki ofensywne w strategii bezpieczeństwa teleinformatycznego

Rozważania na temat tego czy techniki ofensywne mogą być użyte w walce z cyberprzestępcami i czy jest to zgodne z międzynarodowym prawem. Autorzy biorą na analityczny warsztat przykłady cyberataków z Estonii, Gruzji oraz przykłady Stuxneta z 2010 roku i cyberataków, które miały miejsce w Libii w 2011.

http://bit.ly/QtRZgl

Zagrożenia dla sieci energetycznych od strony ataków elektromagnetycznych

Serwis Government Computer News informuje o zagrożeniach teleinformatycznych dla sieci energetycznych w postaci ataków elektromagnetycznych i wzmożonej aktywności słonecznej. Jest to wynik analizy specjalistów amerykańskiego Homeland Security i Departamentu Obrony. Przy okazji lektury artykułu można się dowiedzieć o amerykańskiej propozycji SHIELD Act, która wprowadza propozycję zasad ochrony przed atakiem elektromagnetycznym.

http://bit.ly/PCJuyC

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

Wolność i Bezpieczeństwo

Sławomir Kosieliński
Fundacja Instytut Mikromakro

Konferencja w kręgu pięciu żywiołów

19 września 2012 r. rozpocznie się IX Konferencja „Wolność i bezpieczeństwo". To spotkanie osób zajmujących się tradycyjnie pojmowanym zarządzaniem kryzysowym, jaki i ochroną cyberprzestrzeni.

Na konferencjach z cyklu „Wolność i bezpieczeństwo" magazyn menedżerów i informatyków „Computerworld" popularyzuje wiedzę o zapobieganiu i walce ze współczesnymi żywiołami: wodą, ogniem, powietrzem, ziemią i cyberprzestrzenią. Wydają się one na co dzień bardzo odległe od nas, po czym uderzają w nas z całą mocą i bezwzględnością. Wówczas trzeba umieć nad nimi zapanować zgodnie z zasadami reagowania kryzysowego. W tym roku współorganizatorami przedsięwzięcia – oprócz tygodnika Computerworld są think-tank Fundacja „Instytut Mikromakro" oraz Fundacja Bezpieczna cyberprzestrzeń.

Konferencja po raz pierwszy odbyła się 8 lat temu. Wtedy tematem wiodącym była ochrona tożsamości internauty. W kolejnych latach organizatorzy podejmowali zagadnienia związane z bezpieczeństwem narodowym, ochroną infrastruktury krytycznej, łącznością specjalną, ochroną granic, teleinformatycznym wsparciem akcji przeciwpowodziowych, ale również ochroną cyberprzestrzeni. Tym razem skupimy się na ochronie infrastruktury krytycznej przed cyberatakami oraz na „wojnie dronów" – teleinformatyką na współczesnym polu walki w działaniach jednostek sił specjalnych. Głównym wydarzeniem konferencji będą CYBER EXE POLSKA 2012 – pierwsze w Polsce ćwiczenia z ochrony infrastruktury krytycznej przed atakami cybernetycznymi.

Ćwiczenia z zarządzania kryzysowego na konferencjach „WiB"

Notabene, tradycją tej konferencji jest organizacja pokazów i ćwiczeń z zarządzania kryzysowego. Pierwsze miały miejsce w 2009 r., kiedy zorganizowano pokazy współdziałania służb zarządzania kryzysowego na Zatoce Gdańskiej. Miała wówczas miejsce pozorowana akcja odbijania statku Urzędu Morskiego „Zodiak" z rąk przestępców o skłonnościach terrorystycznych. W akcji wzięli udział funkcjonariusze Morskiego Oddziału Straży Granicznej, Specjalnego Pododdziału Antyterrorystycznego Policji Pomorskiej, śmigłowiec Marynarki Wojennej ANAKONDA i śmigłowiec MOSG, jednostki SAR i WOPR, ratownictwo medyczne Sopotu i Gdańska.

W 2010 r. odbijano znowuż z rąk terrorystów okręt desantowy ORP „Poznań" zacumowany naprzeciwko Wałów Chrobrego w Szczecinie siłami Specjalnego Pododdziału Antyterrorystycznego Policji Zachodniopomorskiej.

Natomiast w 2011 r. przeprowadzono trening współdziałania służb zarządzania kryzysowego podczas ewakuacji hali Ergo Arena w Gdańsku z udziałem studentów i oficerów Akademii Marynarki Wojennej, służb zarządzania kryzysowego Wojewody Pomorskiego, Prezydentów Gdańska i Sopotu oraz przy wsparciu śmigłowca MW RP i LPR.

Co się wydarzy w tym roku? O tym przekonamy się już od środy 19 września do piątku 21 września.

Więcej na:
http://wolnosc2012.computerworld.pl

NEWS

Gartner przewiduje wysokość wydatków na bezpieczeństwo w 2016

Znana firma konsultingowa Gartner przedstawia swoje szacunki dotyczące wydatków na bezpieczeństwo w 2016 roku. Zdaniem Gartnera wydatki te wyniosą ponad 86 mld USD. Wyniki badań Gartnera wskazują na systematyczny wzrosty wydatków na bezpieczeństwo teleinformatyczne od kilku lat.

http://bit.ly/TZ0V0D

Powstał CERT-EU, który ma świadczyć usługi dla instytucji europejskich

Po okresie rocznych testów na dobre ruszył CERT dla instytucji europejskich takich, jak Parlament Europejski, Komisja Europejska itp. Główny wkład w przygotowanie zespołu do gotowości miała Agencja ENISA, która również będzie wspomagała zespół CERT-EU w jego dalszym funkcjonowaniu.

http://bit.ly/PvePVp

Raport McAfee na temat zagrożeń w drugim kwartale 2012 r.

Firma McAfee opublikowała raport o zagrożeniach w sieci w drugim kwartale 2012 roku. Wynika z niego że liczba wirusów cały czas rośnie, w porównaniu do poprzedniego kwartału wzrosła o 23 procent. Szacuje się ze obecnie po Internecie krąży 9
0 milionów wirusów. Autorzy raportu ostrzegają o rosnącej liczba ataków skierowanych na smarfony i tablety. Najchętniej atakowane są urządzenia z systemami Android, dzieje się tak ponieważ po zainfekowaniu wirusem system nie zostaje spowolniony a tym samym użytkownik nie orientuje się że urządzenie zostało zaatakowane. Zachęcamy do zapoznania się z raportem i zainstalowania programu antywirusowego na swoim smartfonie.

http://bit.ly/M70AmW

Cyber-EXE Polska 2012

Zespół planistyczny Cyber-EXE Polska 2012 przy pracy

Foto: IDG Polska

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

W chwili kiedy czytają Państwo ten numer w całym kraju odbywają się, lub dopiero co się zakończyły, pierwsze polskie ćwiczenia z ochrony infrastruktury teleinformatycznej w cyberprzestrzeni. W trakcie koordynowanych z Wrocławia ćwiczeń sprawdzone zostanie przygotowanie i zdolność polskich firm i instytucji na odparcie ataku teleinformatycznego, który w istotny sposób mógłby naruszyć bezpieczeństwo strategicznych zasobów, a skutki tego mogłyby dotknąć obywateli.

Organizatorem ćwiczeń jest Tygodnik Computerworld, Fundacja Instytut Mikromakro oraz Fundacja Bezpieczna Cyberprzestrzeń (koordynator przygotowań i przebiegu ćwiczeń). W ćwiczeniach bierze udział wiele instytucji i firm zarówno z administracji państwowej jaki i sektora prywatnego. Uczestnikiem ćwiczeń są między innymi: Rządowe Centrum Bezpieczeństwa, Ministerstwo Obrony Narodowej, Komenda Główna Policji, OGP Gaz-System SA, operator sieci Orange Polska, PSE-Operator SA.

Ćwiczenia otrzymały wsparcie Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), którzy aktywnie pomagali w przygotowaniach, między innymi organizując specjalne warsztaty dla przygotowujących ćwiczenia (patrz wywiad z Razvanem Gavrila z ENISA).

Przygotowania do ćwiczeń to ponad pół roku pracy kilkunastoosobowego zespołu, składającego się ze specjalistów z wielu instytucji administracji publicznej i sektora prywatnego. Kilkanaście spotkań, praca grup roboczych, przygotowany materiał multimedialny, wydzielone środowisko testowe do przeprowadzenia symulacji ataków, to wszystko wiązało się z intensywną pracą i prawdziwym wyzwaniem dla zespołu CYBER-EXE Polska 2012.

W czasie ćwiczeń przećwiczymy reakcję na kilkadziesiąt najróżniejszych zdarzeń będących zagrożeniem dla bezpieczeństwa. Współdziałać ze sobą będzie kilkadziesiąt podmiotów, które są odpowiednikami komórek organizacyjnych, stanowisk lub nawet całych instytucji. Jest to z pewnością duże wyzwanie logistyczne. Oczekujemy jednak, że podjęte starania i wysiłek są jak najbardziej uzasadnione, gdyż spodziewamy się bardzo istotnych wniosków i obserwacji, które mamy nadzieję, że w istotny sposób wzbogacą system reagowania na najpoważniejsze naruszenia bezpieczeństwa w „polskiej cyberprzestrzeni", o których rzecz jasna napiszemy już w następnym numerze CIIP focus.

CYBER-EXE POLSKA 2012

Cele ćwiczeń przygotowane przez RCB są następujące:

- *Sprawdzić **ZDOLNOŚĆ DO REAKCJI** na atak teleinformatyczny 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*

ĆWICZENIA BUDUJĄ ZAUFANIE

Z ekspertami Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), o ich organizacji, o ćwiczeniach z zakresu cyberbezpieczeństwa i korzyściach z nich płynących rozmawia Redakcja CIIP focus.

Razvan Gavrila podczas szkolenia dla zespołu Cyber-EXE Polska 2012 foto IDG Polska

CIIP Focus: Czym jest ENISA? Kiedy została założona i jakie są jej główne zadania?

ENISA: Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) została założona w 2004 roku. Jest agencją Unii Europejskiej, a jej zadania, zostały określone w przepisach założycielskich i są uszczegóławiane w corocznym programie pracy. Ogólnie rzecz biorąc, zadania można podzielić na cztery grupy tematyczne:

• Think tank: przygotowywanie raportów dotyczących praktyk z obszaru bezpieczeństwa w Europie i pojawiających się zagrożeń (np. cloud computing).
• Wspieranie państw członkowskich (na przykład wspieranie tworzenia i szkolenie zespołów CERT lub planowania, przeprowadzanie i ocena ćwiczeń cybernetycznych).
• Ułatwianie współpracy transgranicznej (na przykład poprzez wspieranie ogólnoeuropejskich ćwiczeń z zakresu bezpieczeństwa cybernetycznego).
• Zapewnienie spójnego ogólnoeuropejskiego podejścia (na przykład poprzez wspieranie implementacji artykułu 13a z pakietu telekomunikacyjnego).

- Kiedy ćwiczenia z cyberbezpieczeństwa stały się ważne dla ENISA i jakie są dotychczasowe doświadczenia z nimi związane? Dlaczego są one tak ważne dla Agencji?

- Komunikat Komisji z 2009 roku, w sprawie ochrony krytycznej infrastruktury informatycznej, „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności", był podstawą dla zwrócenia większej uwagi na ćwiczenia z zakresu cyberbezpieczeństwa w Europie.
Dotychczasowe działania w tym obszarze wykazały, że w Europie istnieje szereg podejść do tematu ćwiczeń i zagadnienia odporności. Wsparcie, które ENISA może zapewnić w tym obszarze jest powszechnie wykorzystywane przez państwa członkowskie. Zarówno ćwiczenia krajowe, jak i międzynarodowe, wspierane lub wspomagane przez ENISA okazały się sukcesem i źródłem cennych doświadczeń, które przyczyniły się do dalszej poprawy odporności i współpracy kryzysowej w sytuacji zagrożeń cybernetycznych. Transgraniczny charakter cyberzagrożeń i krytycznych infrastruktur informatycznych, jak również rosnące uzależnienie nowoczesnego społeczeństwa od technologii i systemów informatycznych, sprawia, że jest to obszar priorytetowy dla ENISA. Więcej informacji na temat ćwiczeń cybernetycznych i działań z zakresu współpracy ENISY można znaleźć pod adresem: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation

- Czy ćwiczenia Cyber Europe 2012 są inne niż Cyber Europe 2010? Jeśli tak, to jakie są główne różnice?

- Ćwiczenia Cyber Europe 2012 opierają się na doświadczeniach zdobytych w czasie Cyber Europe 2010. Podczas tegorocznych ćwiczeń będą testowane operacyjne procedury współpracy w sytuacji kryzysowej związanej z cyberprzestrzenią, które zostały opracowane w wyniku ćwiczeń Cyber Europe 2010. Ponadto, jednym z zaleceń Cyber Europe 2010 było zaangażowanie sektora prywatnego w ćwiczeniach cybernetycznych, co będzie miało miejsce w czasie

logo:http://www.enisa.europa.eu

ćwiczeń w tym roku.

- Jak państwa członkowskie mogą otrzymać wsparcie ENISA w organizowaniu ćwiczeń?

- ENISA dzieli się swoimi doświadczeniami w organizowaniu i przeprowadzaniu ćwiczeń z państwami członkowskimi oraz organizuje dla nich seminaria. Ponadto, na życzenie oferuje inne rodzaje wsparcia dla państw członkowskich i instytucji UE w zakresie planowania ćwiczeń cybernetycznych. Wreszcie ENISA pomaga w planowaniu i przeprowadzaniu ćwiczeń regionalnych i ogólnoeuropejskich.

- Jakie są najbardziej interesujące doświadczenia zgromadzone po zorganizowanych do tej pory w Europie ćwiczeniach?

- Żeby wymienić tylko kilka z nich:
• Ważne jest, aby przeszkolić uczestników przed ćwiczeniem, co potęguje wartość dydaktyczną ćwiczenia.
• Ćwiczenia są doskonałym narzędziem służącym budowaniu zaufania.
• Wpływ mniejszych ćwiczeń pomiędzy krajami może potencjalnie prowadzić do lepszej współpracy w Europie jako całości.

- Co jest kluczowe w fazie planowania ćwiczenia?

- Stworzenie dedykowanego i konstruktywnego zespołu planistycznego, jasne określenie od początku celów, przeznaczenie wystarczająco dużo czasu na etap planowania, a nie tylko skupianie się na scenariuszu, ponieważ istnieją inne ważne kwestie, takie jak ewaluacja ćwiczenia, szkolenie uczestników itp.

- Co organizatorzy ćwiczeń krajowych powinni uwzględnić podczas ćwiczeń?

- Organizatorzy powinni upewnić się, że wszyscy rozumieją swoją rolę (moderatorzy, uczestnicy lub obserwatorzy), oraz że ćwiczenie przebiega w odpowiednim tempie. Ponadto, nie powinni zapominać, że końcowym wynikiem ćwiczenia jest dopiero ocena dokonana w ramach fazy ewaluacji, tak więc kluczowe jest gromadzenie w czasie ćwiczenia danych, które pomogą stwierdzić, czy ćwiczenie spełniło założone cele. Wreszcie, organizatorzy powinni podejmować decyzje i działania, na podstawie celów ćwiczenia.

- Jak wykorzystać ćwiczenia cybernetyczne do budowania lepszego partnerstwa publiczno-prywatnego? Czy ćwiczenia mogą w tym pomóc?

- Jednym z celów ćwiczenia Cyber Europe 2010 było budowanie zaufania. 95% państw członkowskich uznało, że ćwiczenie ten cel osiągnęło (por. sprawozdanie końcowe z CE 2010 dostępne na stronie internetowej ENISA). To, że istnieje co najmniej jeden punkt kontaktowy z każdego kraju, którego reprezentant regularnie spotyka się, wymienia informacje i współpracuje z pozostałymi, było prawdopodobnie najważniejszym środkiem budowy zaufania w ramach ćwiczeń. Stało się jasne, że uczestnicy oprócz wymiany informacji i poglądów zaczęli budować wspólne zaufanie już poprzez samo spotykanie swoich odpowiedników. To był przykład budowania zaufania pomiędzy państwami, ale jest prawdopodobne, że podobne rezultaty można osiągnąć pomiędzy organizacjami publicznymi i prywatnymi, które wspólnie będą pracować nad określonym projektem. Zobacz także działania ENISA w sprawie partnerstwa publiczno-prywatnego: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps

- Czy ENISA prowadzi badania nad istniejącymi i przyszłymi zagrożeniami cybernetycznymi? Jakie problemy w sferze bezpieczeństwa IT czekają nas w najbliższej przyszłości?

- ENISA nie jest organizacją badawczą. Agencja działa na rzecz poprawy ogólnego poziomu bezpieczeństwa sieci i informacji w Unii Europejskiej. Ponieważ nasze społeczeństwo stało się uzależnione od ICT, ochrona krytycznej infrastruktury informatycznej oraz aplikacji, które działają w oparciu o nią, nie tylko sprowadza się do technologii i bezpieczeństwa, ale jest ściśle związana z konkurencyjnością UE i jej dobrobytem. Podczas gdy nowe technologie i modele biznesowe (od mediów społecznych, cloud computing-u do inteligentnych sieci) przyniosły wiele korzyści, ich użytkowaniu towarzyszy rozwój nowego zestawu zagrożeń cybernetycznych, które rozwijają się w coraz bardziej gwałtowny, wyrafinowany i złowieszczy sposób. Dlatego ENISA śledzi prowadzone badania nad przyszłymi zagrożeniami, co pomaga również w przygotowywaniu przyszłych ćwiczeń cybernetycznych.

- Dziękuję za rozmowę.

Zespół ENISY ds. Cyber Ćwiczeń
Wydział ds. CIIP i Odporności:

Panagiotis Trimintzios
Ekspert ds. Bezpieczeństwa Sieci i Informacji
Maj Ritter Klejnstrup
Specjalista ds. Bezpieczeństwa Informacji i Komunikacji
Razvan Gavrila
Ekspert ds. Bezpieczeństwa Sieci i Informacji

Rozmowę przeprowadzili Maciej Pyznar - Rządowe Centrum Bezpieczeństwa i Mirosław Maj – Fundacja Bezpieczna Cyberprzestrzeń.

Niniejszy artykuł jest drugim z serii artykułów dotyczących zespołów CERT. W pierwszym numerze poruszaliśmy temat historii powstania i zakresu działania zespołów typu CERT. W następnych publikacjach poruszane będą tematy polskiego środowiska CERT-owego, zasad funkcjonowania zespołów typu CERT, używanych przez nie narzędzi, współpracy krajowej i międzynarodowej.

C E R T

Zasady tworzenia zespołu reagowania. Cztery pierwsze kroki.

Mirosław Maj

Fundacja Bezpieczna Cyberprzestrzeń, ComCERT SA

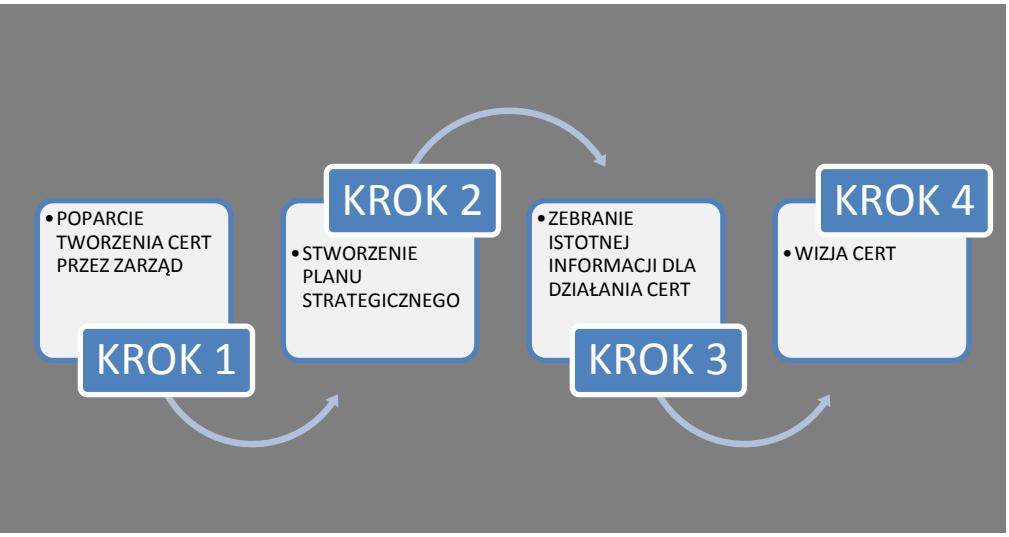
Wiele osób nie do końca rozumie sens tworzenia oddzielnej komórki organizacyjnej, która miałaby się zajmować tylko i wyłączenie sprawami reagowania na incydenty sieciowe. W rozumieniu wielu „dowodzących" tymi sprawami powinien się zająć departament informatyki, no może w najlepszym przypadku organizacyjna komórka bezpieczeństwa, jeśli takowa powstała. W organizacji może istnieć bardzo skomplikowana struktura organizacyjna działów biznesowych i nie budzi to niczyjego zdziwienia, ale w tej samej organizacji może być całkowity brak zrozumienia dla rozdziału funkcji zarządzania informatyką i zapewnienia jej bezpieczeństwa, a co dopiero od wydzielenia jeszcze bardziej specjalistycznej komórki jaką jest komórka reagująca na przypadki naruszenia bezpieczeństwa teleinformatycznego. Czasami dopiero poważny incydent obnaża słabości funkcjonującej struktury i zmusza do poważnego pomyślenia o zmianach.

Oczywiście nie warto czekać na takie przypadki tylko wcześniej pomyśleć o pozytywnych zmianach. Jak to zrobić? W sukurs przychodzą nam dobre praktyki, które w ciągu dwudziestu kilku ostatnich lat wypracował „świat CERT-owy". Jedną z takich dobrych praktyk jest metodyka stworzona przez wspominany już na łamach CIIP focus – pierwszy w świecie CERT, czyli amerykański CERT Coordination Center [(1)].

Od czego więc zacząć budowę CERT-u?

KROK 1 – POPARCIE TWORZENIA CERT PRZEZ ZARZĄD

Okazuje się, że przynajmniej na początku „projekt CERT" niewiele różni się od innych projektów, czyli potrzebne jest nam **„błogosławieństwo" z góry**. Ktoś spośród odpowiedzialnych za funkcjonowanie organizacji powinien sam zaproponować takie rozwiązanie lub zostać przez kogoś do tego namówiony. Ta pierwsza opcja to rzecz jasna sytuacja bliska ideału, niestety rzadko spotykana. Dlatego raczej trzeba postawić na drugie. Kto to wykona? Potrzebny nam jest **entuzjasta CERT**, czyli osoba która nie tylko będzie przekonana do idei CERT, ale również ta idea najzwyklej w świecie takiej osobie się spodoba. Praktyka pokazuje, że zespoły CERT-owe najlepiej rozwijają się tam gdzie właśnie taki entuzjasta, a jeszcze lepiej – grupa entuzjastów się pojawi. Może się wtedy okazać, że znacznie sprawniejsze i efektywniejsze zespoły powstają w mniejszych organizacjach, wcale nie dysponujących wielkimi budżetami. Osobiście znam z bliska historie i realia działania kilku firm z samej góry polskich rankingów biznesowych, w których nie sposób kadrę średniego szczebla kierowniczego nakłonić do stworzenia zespołu CERT. Sam fakt, że polskie środowisko operatorów telekomunikacyjnych doczekało się raptem dwóch formalnie istniejących zespołów CERT, jest najlepszym tego świadectwem. Zresztą podobnie jest ze środowiskiem bankowym, w którym co prawda istnieją zespoły bezpieczeństwa, ale CERT (w tym wypadku CSIRT) jest tylko jeden. Oczywiście w poparciu „z góry" nie chodzi tylko i wyłącznie o dobre słowo. Ważne jest aby przychylne spojrzenie na chęć budowania CERT związane było z zapewnieniem odpowiedniego wsparcia kompetencyjnego w tym działaniu oraz zapewnieniem odpowiedniego budżetu.



KROK 2 – STWORZENIE PLANU STRATEGICZNEGO

Jeśli mamy już poparcie z góry to czas przygotować odpowiedni plan budowy CERT. **Co powinien taki plan zawierać?** Po pierwsze ramy czasowe powstania CERT-u, po drugie organizację grupy osób, która zajmie się projektem, po trzecie strategię komunikacji z resztą organizacji, po czwarte ustalenie metod pracy w ramach zespołu tworzącego CERT. Myśląc o planie strategicznym nie powinniśmy myśleć o biurokratycznym podejściu i produkcji kilogramów doku-

(1) http://www.cert.org/csirts/Creating-A-CSIRT.html

mentacji. Chodzi raczej o gruntowną i uczciwą analizę tego jak zabrać się za budowę CERT-u, jakie potrzebne są zasoby, ile mamy czasu na budowę i jak będziemy pracować w tym projekcie. Najistotniejsze z tego jest stworzenie dobrego zespołu projektowego. Zebranie ludzi, których już wcześniej określiliśmy mianem entuzjastów. Warto takich osób poszukać. Może się okazać, że znajdują się one na „drugim biegunie" organizacji. Często wiele zespołów CERT-owych rozpoczyna swoją działalność od funkcjonowania tzw. „zespołu wirtualnego". Osoby będące członkami CERT nie tworzą formalnej komórki organizacyjnej w strukturach. Są grupą specjalistów, którzy pracują w różnych komórkach organizacyjnych, a tylko w razie potrzeby jednoczą siły aby rozwiązać problem bezpieczeństwa zaistniały w wyniku incydentu bezpieczeństwa. Jest to rozwiązanie warte uwagi w sytuacji kiedy takich przypadków jest niewiele, a jednocześnie potrzebne są najróżniejsze kompetencje w celu rozwiązaniu problemu. Trudno byłoby znaleźć osobę posiadającą wszystkie te kompetencje.

Najczęściej „zespoły wirtualne" migrują w kierunku struktury formalnej. Tak było na przykład w przypadku pierwszego polskiego CERTu – zespołu CERT Polska. Rozpoczął on funkcjonowanie w 1996 roku jako „zespół wirtualny" pod nazwą CERT NASK, a dopiero w 2001 roku pojawił się w strukturach organizacyjnych NASK jako zespół CERT Polska z pełnoetatowymi pracownikami.

Koncepcja „zespołu wirtualnego" i szukanie specjalistów-entuzjastów, sprawia że warto budowanie CERT-u ogłosić dość wcześnie. Być może jest to pomysł na wewnętrzną rekrutacją i szansa dla wielu pracowników na awans zawodowy w interesującej ich dziedzinie. Sam rynek pracy nie oferuje wielu specjalistów, którzy ściśle mieliby się zajmować takimi zagadnieniami i rekrutacja do zespołu może być dość trudnym zadaniem.

KROK 3 – ZEBRANIE ISTOTNEJ INFORMACJI DLA DZIAŁANIA CERT

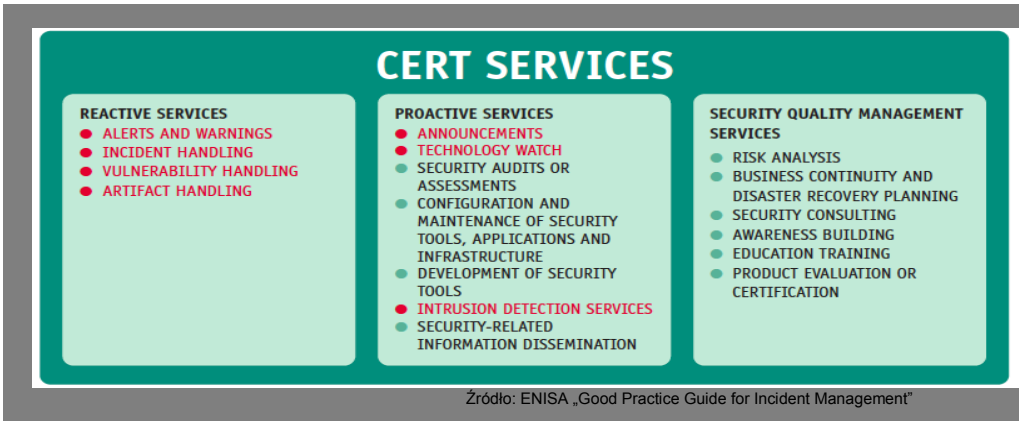
A co to jest istotna informacja dla działania CERT? Brzmi to dość enigmatycznie, a sprawa jest stosunkowo prosta. Chodzi o to co w praktyce CERT miałby robić. Źródła tej wiedzy są praktycznie dwa. Pierwsze jest bardzo naturalne. Jest to po prostu zestaw tych działań, na które w organizacji pojawiło się zapotrzebowanie. Czyli jak są sprawy związane z tym, że ktoś atakuje nasz serwer WWW, to to jest istotna informacja dla przyszłego działania CERT – trzeba takie przypadki obsługiwać. Jeśli ktoś pyta co robić po tym jak zauważył działanie wirusa na swoim komputerze, to takim incydentem wewnętrznym też może zajmować się CERT. Przypadki takie albo będą oczywiste, albo wystarczy mała „burza mózgów" wśród zainteresowanych, aby je wyłapać. Ta sama „burza mózgów" może się przerodzić w obrady na temat tego co innego, oprócz tych pojawiających się zgłoszeń, mógłby robić CERT? Tu do pomocy przyda się nam zestaw potencjalnych serwisów CERT-owych (patrz rysunek poniżej). Postępowanie jest w praktyce dość proste. Bierzemy usługi CERT-owe punkt po punkcie i zastanawiamy się, czy powinniśmy je świadczyć. Bardziej zaawansowanym rozwinięciem tego zadania jest przeprowadzenie dodatkowej ankiety wśród przyszłych pracowników CERT. Zawierać ona może dwa proste pytania w stosunku do każdej z usług: 1) W jakim stopniu jesteśmy przygotowani do jej świadczenia? 2)Czy nasz klienci (tzw. CERT *constituency*) oczekuje od nas świadczenia takiej usługi. Wyniki ankiety mogą okazać się bardzo istotną podpowiedzią do dalszego działania. Jeśli na naszej liście znajdziemy takie usługi, które nie dość, że jesteśmy przygotowani już świadczyć t są jeszcze dodatkowo bardzo oczekiwane przez naszych klientów, to rzecz jasna te pozycje stają się pewniakami na naszej liście usług. Jeśli coś jest bardzo oczekiwane, a my słabo jesteśmy przygotowani do zaproponowania tego, to czas na edukację lub wzmocnienie siły zespołu dodatkowymi specjalistami. W takiej sytuacji po powinniśmy też krytycznie spojrzeć na to co bardzo dobrze już potrafimy, ale wcale nie jest oczekiwane. Albo z tego zrezygnujmy, albo przekonajmy nasze *constituency* do swojego zmiany punktu widzenia i zainteresowań.

KROK 4 WIZJA CERT

Wizja CERT to w praktyce zestaw pod tytułem: końcowy zestaw serwisów, misja działania, obszar funkcjonowania (tzw. *constituency*), wybór modelu organizacyjnego, identyfikacja zasobów technicznych, zapewnienie budżetu dla CERT.

O serwisach i modelu organizacyjnym już wspomniałem wcześniej. Budżet rozumie się sam przez się – warto o niego zadbać już na etapie pozyskania wsparcia od zarządu. Natomiast jeśli chodzi o *constituency*, to trzeba pamiętać, że CERT pełni służebną rolę wobec niego. Krótko mówiąc ma pomagać użytkownikom sieci objętej ochroną CERT-u w rozwiązywaniu problemów już na etapie odpierania ataków sieciowych, a przede wszystkim być pomocnym w likwidacji skutków tych ataków. Ważne jest aby użytkownik miał zaufanie do swojego CERT-u. Nie może on się bać zgłaszać incydentu. Takie zaufanie należy budować od samego początku. Znane są przypadki karygodnych błędów w tej dziedzinie – na przykład CERT publikuje raport dostępny publicznie, w którym użytkownik może przeczytać o … zgłoszonym przez siebie przypadku i swojej osobie „z imienia i nazwiska". Czy taki użytkownik w przyszłości zgłosi jeszcze problem do swojego CERT-u? Pytanie raczej retoryczne.

Mirosław Maj – specjalista bezpieczeństwa teleinformatycznego. Fundator i prezes Fundacji Bezpieczna Cybeprzestrzeń. Wiceprezes spółki ComCERT SA, a w przeszłości wieloletni kierownik zespołu CERT Polska. Od wielu lat ściśle współpracuje z Agencją ENISA współtworząc publikacje na temat bezpieczeństwa teleinformatycznego i pracując w grupach roboczych. Koordynator pierwszych polskich ćwiczeń z ochrony w cyberprzestrzeni – Cyber-EXE Polska 2012



Źródło: ENISA „Good Practice Guide for Incident Management"

Bezpieczeństwo systemów sterowania, po serii incydentów związanych z atakami wirusowymi na infrastrukturę techniczną w Iranie, trafiło na pierwsze strony gazet. Analiza ataków za pomocą Stuxnet i Duqu, maluje obraz, zgodnie z którym wojny, terroryzm i przestępstwa realizowane będą głównie w cyberprzestrzeni, a poprzez zakłócenie działania informatycznych systemów sterowania infrastrukturą krytyczną ich skutki przeniosą się bezpośrednio na społeczeństwa i obywateli. Istnieją metody, dzięki którym jest możliwe ograniczenie negatywnego wpływu działania złośliwego oprogramowania na tą infrastrukturę, ale by z nich skorzystać, musimy poznać dokładnie swoje systemy Scada. Zanim ktoś obcy zrobi to za nas…

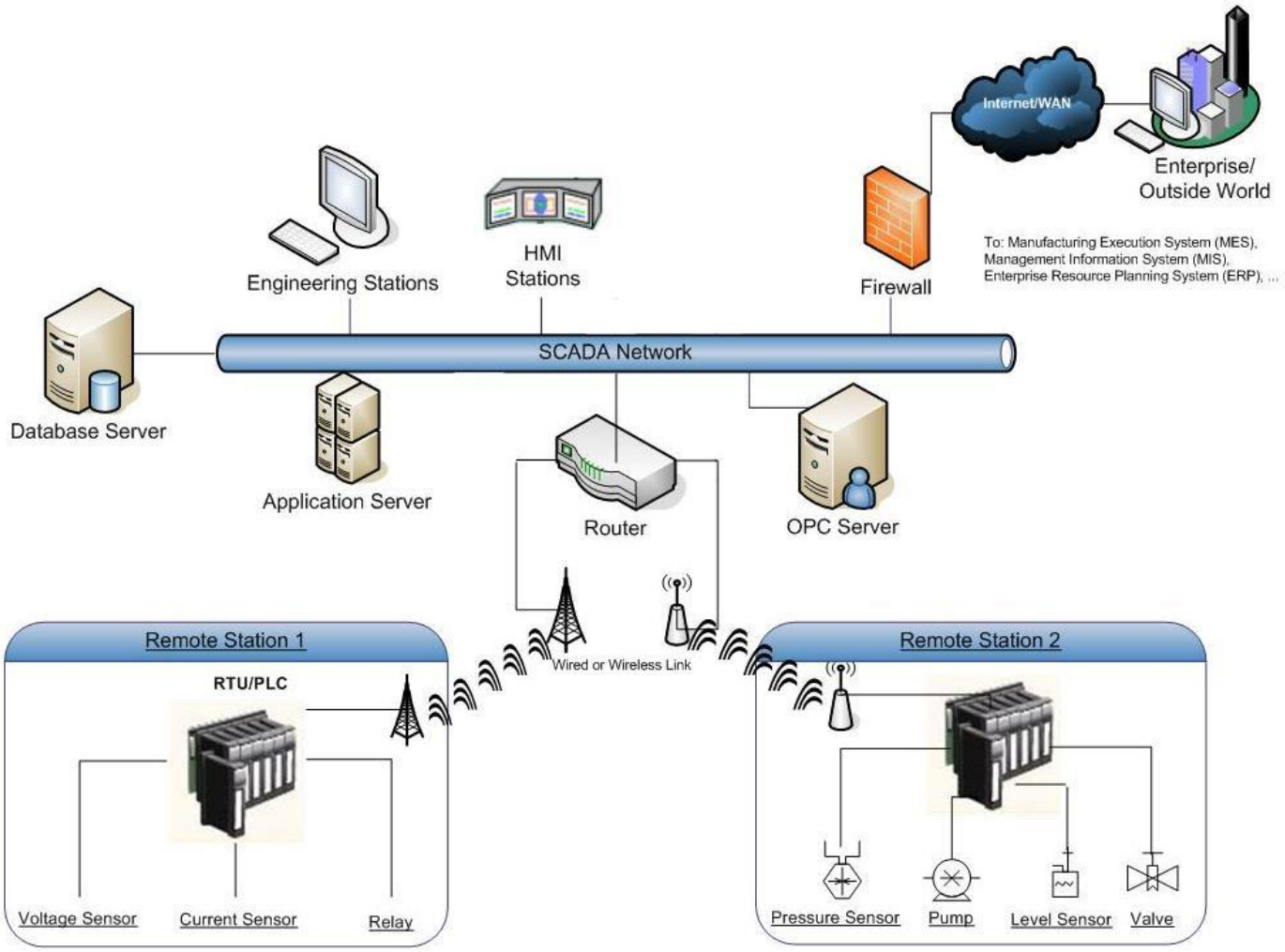
SCADA

cyberbezpieczeństwo systemów sterowania

Tadeusz Włodarczyk
PSE Operator SA

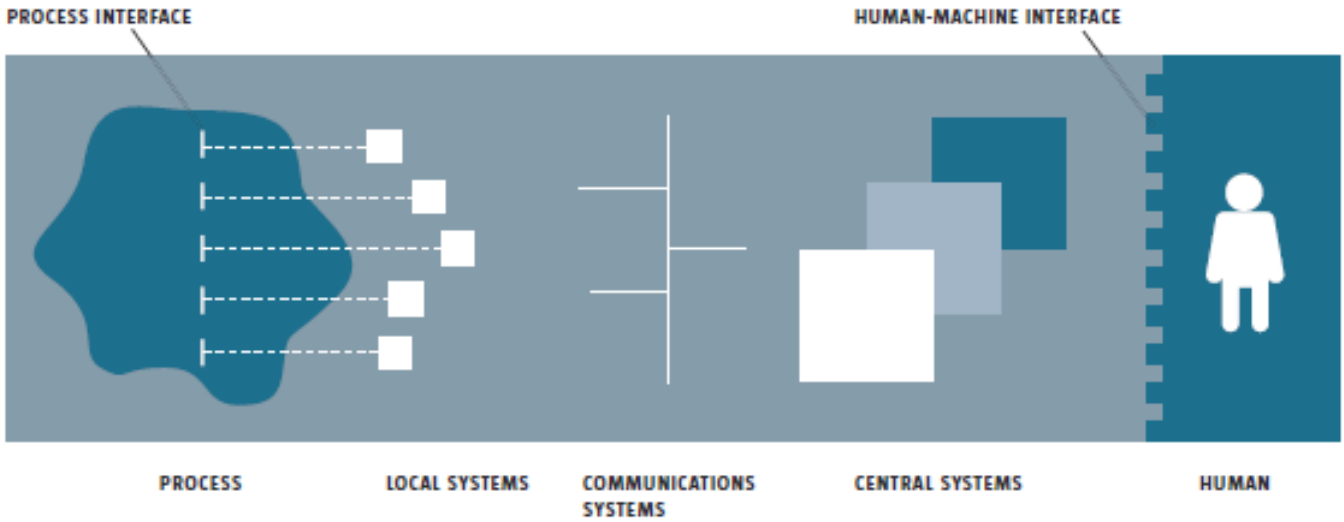
Zgodnie z tezą ze wstępu, w celu opracowania skutecznego systemu bezpieczeństwa, składającego się z zestawu procedur eksploatacyjnych oraz zabezpieczeń technicznych i programowych, należy najpierw dogłębnie poznać infrastrukturę chronionego systemu Scada. Cała bowiem przewaga właściciela tej infrastruktury nad potencjalnym cyber napastnikiem polega na tym, że posiada nieograniczony i pełny dostęp do informacji o jej budowie i działaniu. Praktyczne wykorzystanie tej wiedzy w trakcie opracowywania i wdrażania zabezpieczeń pozwoli na implementację skutecznych metod wykrycia ataku w pierwszej jego fazie, to jest w momencie, w którym dokonywane jest rozpoznawanie zaatakowanego systemu. Należy stanowczo stwierdzić, iż skuteczna obrona przed infekcją złośliwym oprogramowaniem, mającym na celu na zakłócenie pracy systemów teleinformatycznych jako takich, nie jest już dziś możliwa, prace osób i firm tworzących systemy bezpieczeństwa skupiają się co najwyżej na zmniejszaniu prawdopodobieństwa przeprowadzenia ataku oraz eliminacji wystąpień przypadkowych awarii, przy czym wszyscy mają świadomość, iż prawdopodobieństwo to nigdy nie będzie równe 0%. Zaawansowane ataki typu APT (Advanced Persistent Threat), wykorzystujące biały wywiad, socjotechnikę oraz coraz częściej podatności systemów typu „zero day", dają 100% skuteczność dostarczenia złośliwego kodu w pożądane miejsce.

Scada (ang. Supervisory Control And Data Acquisition – system sterowania, kontroli i akwizycji danych) jest systemem nadrzędnym w stosunku do urządzeń sterowników PLC (ang. Programmable Logic Controller) oraz wykonawczych i pomiarowych RTU (ang. Remote Terminal Unit), użytkowanych do automatyzacji procesów technologicznych w produkcji, przesyle, teletransmisji, kolei, medycynie i innych dziedzinach gospodardki. Głównymi komponentami Scady są moduły: zbierania danych o stanie urządzeń PLC i RTU (pomiarów), wizualizacji tych stanów na terminalach HMI (ang. Human-Mahcine Interface), sterowania pracą urządzeń oraz procesami technologicznymi opartymi na działaniu tych urządzeń, alarmowania oraz archiwizacji danych. Poniższy schemat obrazuje logiczną budowę Scady:



OpenControl SCADA Network Architecture

Oraz funkcjonalnie poniższy:



Budowa systemów Scada ewoluowała w czasie od lokalnych, w których stacja sterowania i nadzoru HMI była podłączona bezpośrednio do urządzeń sterowników i wykonawczych, do całkowicie sieciowych, gdzie komunikacja pomiędzy HMI a PLC może być realizowana za pośrednictwem sieci publicznej Internet. W toku rozwoju wykształcił się trzy główne generacje systemów:

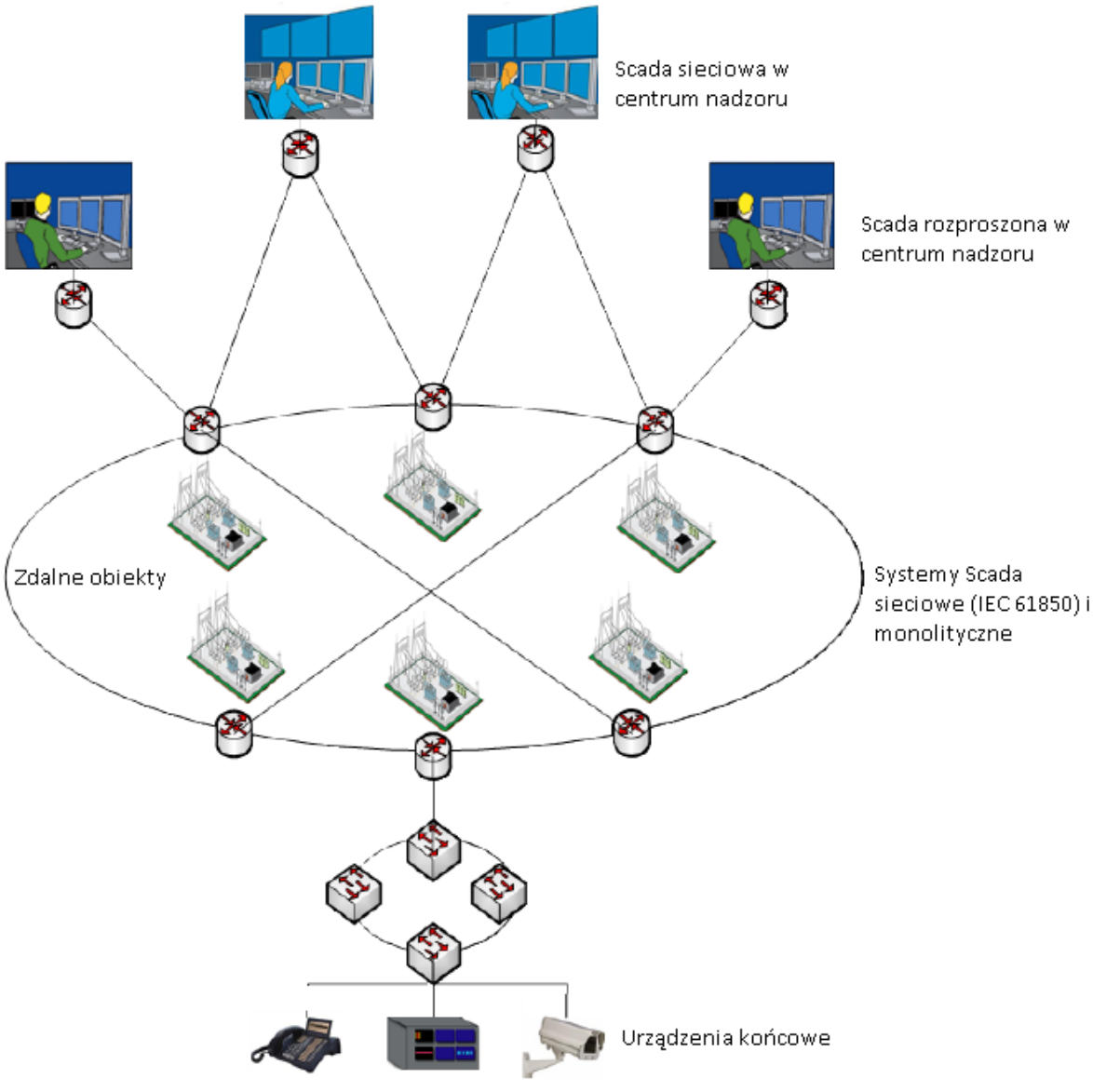
- monolityczna: wszystkimi urządzeniami RTU w systemie, niezależnie od ich lokalizacji, zarządza pojedynczy komputer (dawniej superkomputer typu mainframe), urządzenia są podłączone bezpośrednio do koncentratora portów, będącego składnikiem komunikacyjnym superkomputera. Wymiana danych oparta jest na zastrzeżonych dla poszczególnych producentów systemów Scada i urządzeń RTU protokołach, wykorzystanie publicznej sieci teletransmisji ogranicza się do korzystania ze dzierżawionych kanałów. Bezpieczeństwo systemów zapewniane było poprzez ich izolację od sieci publicznej oraz małą dostępność

wiedzy na temat ich działania;

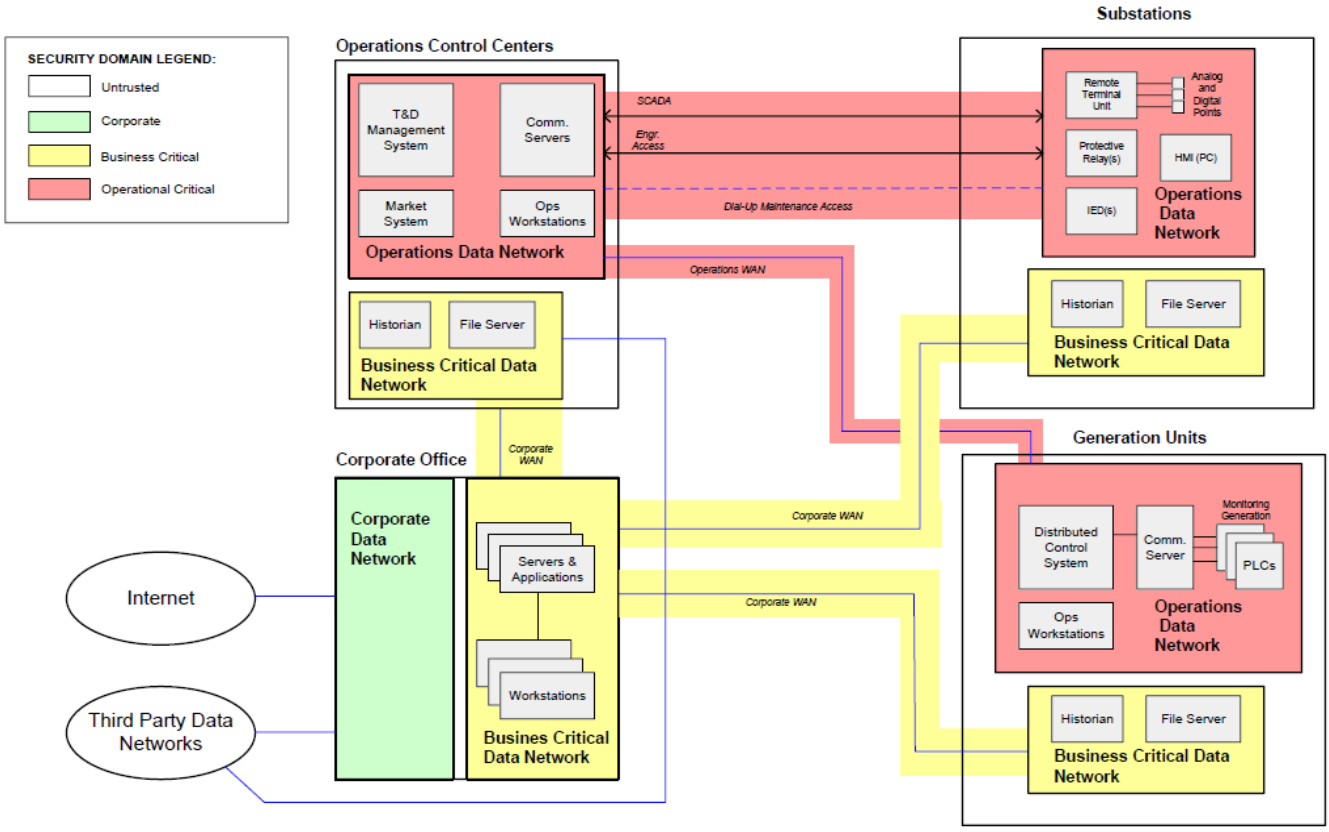
- rozproszona: względy ekonomiczne powodują, iż zarządzanie infrastrukturą jest centralizowane, a systemy monolityczne funkcjonujące na obiektach zdalnych podłączane są za pomocą pojedynczych (lub redundantnych) kanałów w publicznej sieci telekomunikacyjnej do jednego centrum nadzoru. Scady monolityczne rozbudowywane są o moduły komunikacyjne porozumiewające się z systemami centralnymi w oparciu o otwarte i zestandaryzowane protokoły (typu IEC103, ICCP). Powszechnie wykorzystywany jest protokół TCP/IP. Izolacja systemów stawała się pozorna, nadal jednak do budowy systemów Scada wykorzystywano specjalizowane komponenty programowe i techniczne, co w sposób znaczny ograniczało liczbę osób posiadających wystarczającą wiedzę, by zakłócić pracę tych systemów.

- sieciowe: w systemach tych nie występują już dedykowane kanały komunikacyjne pomiędzy systemem Scada a PLC, transmisja danych sterowania i pomiarowych odbywa się wyłącznie z wykorzystaniem protokołu TCP/IP w sieciach LAN/WAN, w tym również sieci publicznej Internet. Do budowy systemów używa się standardowych komponentów sprzętowych i programowych, odchodząc od stosowania rozwiązań dedykowanych, co przyczynia się do zwiększenia ilości osób posiadających wiedzę o ich budowie. Postępują prace standaryzacyjne nad zbudowaniem zasad bezpieczeństwa, w głównej mierze skoncentrowane na zapewnieniu ciągłości działania, będącej najważniejszym parametrem jakościowym systemów sterowania Scada. Nie można już mówić o fizycznej izolacji systemów, gdyż powszechne są połączenia tych systemów do innych sieci (domenowych, publicznej Internet), których bezpieczeństwo zapewniane jest poprzez logiczną separację za pomocą urządzeń firewall, IPS etc.

W związku z faktem, iż systemy technologiczne i infrastruktura krytyczna nadzorowane przez Scady budowane są z przeznaczeniem pracy przez bardzo długi okres, można spotkać dziś każdą z wymienionych powyżej generacji systemów Scada. Co więcej, systemy te są ciągle modernizowane w celu włączenia ich do centralnych systemów nadzoru i sterowania. W skutek ww. obecna typowa topologia systemu Scada wygląda, jak na poniższym rysunku:



Szczególnie ważnym elementem obecnego systemu Scada są systemy centralne nadzoru i sterowania. Ich wielomodułowa budowa, powiązania komunikacyjne do systemów zdalnych (w oddalonych lokalizacjach), interfejsy do systemów biznesowych i sieci publicznej Internet wymagają dogłębnej analizy, do której można wykorzystać poniższy schemat:



Składnikami centralnego systemu Scada są obecnie standardowe rozwiązania świata informatyki: systemy operacyjne, bazy danych, webserwery i aplikacje. W zastosowaniach biznesowych powyższe komponenty sprawdzają się doskonale, dzięki dostosowanemu do potrzeb biznesu cyklowi życia i wprowadzania zmian. Równocześnie ich użytkowanie w środowisku Scada, stawiającego najwyższy priorytet na zachowanie ciągłości działania, jest główną przyczyną problemów z zapewnieniem bezpieczeństwa tych systemów. Nie można bowiem swobodnie aktualizować tych systemów i oprogramowania, gdyż oznacza to konieczność odstawiania systemów od pracy. Oczywiście ma to bezpośredni wpływ na bezpieczeństwo działania tych systemów, dziś bowiem do spowodowania zakłócenia ich pracy wystarczy wykorzystanie dowolnego, w miarę nowego eksploita, który pozwoli na przejęcie kontroli nad jednym z popularnych komponentów (system operacyjny, baza danych, web serwer) z uprawnieniami administratora, lub po prostu wyłączy go z pracy.

Pora zatem odpowiedzieć sobie na pytanie, gdzie w takim razie tkwi przewaga nad napastnikiem, dzięki której możliwe jest chronienie Scady przed cyber zagrożeniami?

Skoro architektura systemów Scada jest bardzo stabilna, zmiany wykonywane są rzadko i wymagają długiego okresu przygotowań i prób, to poprawnie zaprojektowane systemy bezpieczeństwa mają szansę służyć równie długo, jak chronione przez nie systemy. Jest to możliwe wówczas, gdy zabezpieczenia zostaną dobrane do środowiska, w którym będą funkcjonowały. Na dynamicznie zmieniających się brzegach systemów Scada należy budować systemy bezpieczeństwa potrafiące nadążać za ciągle rosnącą ilością podatności (IPS, antywirus, antymalware), a w ich statycznym wnętrzu potrafiące wykryć każde niepożądane lub nieznane działanie (honeypot, SIEM).

Podejście to jest możliwe do wdrożenia pod warunkiem, gdy podejmie się trud poznania rzeczywistych kanałów komunikacyjnych systemów Scad, rodzajów transportowanych tam danych, a na tej podstawie przemodelowania infrastruktury komunikacyjnej systemu Scada. Należy zaprzestać używać stwierdzeń, iż stosowana jest izolacja systemów, i przystąpić do budowy scentralizowanych, wyposażonych w infrastrukturę bezpieczeństwa, węzłów wymiany danych z systemami zewnętrznymi. Często jest to trudne do zrealizowania, gdyż na przestrzeni lat i wraz ze zgłaszaniem przez użytkowników coraz to nowych potrzeb, tych kanałów komunikacyjnych powstało wiele i w różnych technologiach. Powszechnie stosowane są rozwiązania, takie jak VPN (ang. Virtual Private Network), RDP, proxy, SSL, łącza dedykowane, APN. Szczególne niebezpieczeństwo niesie za sobą bezgraniczne zaufanie, jakim darzona jest obecnie technologia VPN, która w rzeczywistości przenosi wszystkie zagrożenia z łączącej się do systemu Scada stacji końcowej, a w skutek szyfrowania transmisji uniemożliwiająca zadziałanie jakichkolwiek zabezpieczeń,. Odkąd powszechny jest protokół https, idea budowania DMZ (ang. DeMilitarized Zone) jako bezpiecznego styku z siecią publiczną Internet stała się dziurawa, gdyż w szyfrowanym kanale przenoszą się dowolne zagrożenia, nie można więc również ufać w bezpieczeństwo stacji końcowych w sieciach LAN przedsiębiorstwa.

Rekomendowaną architekturą komuni-

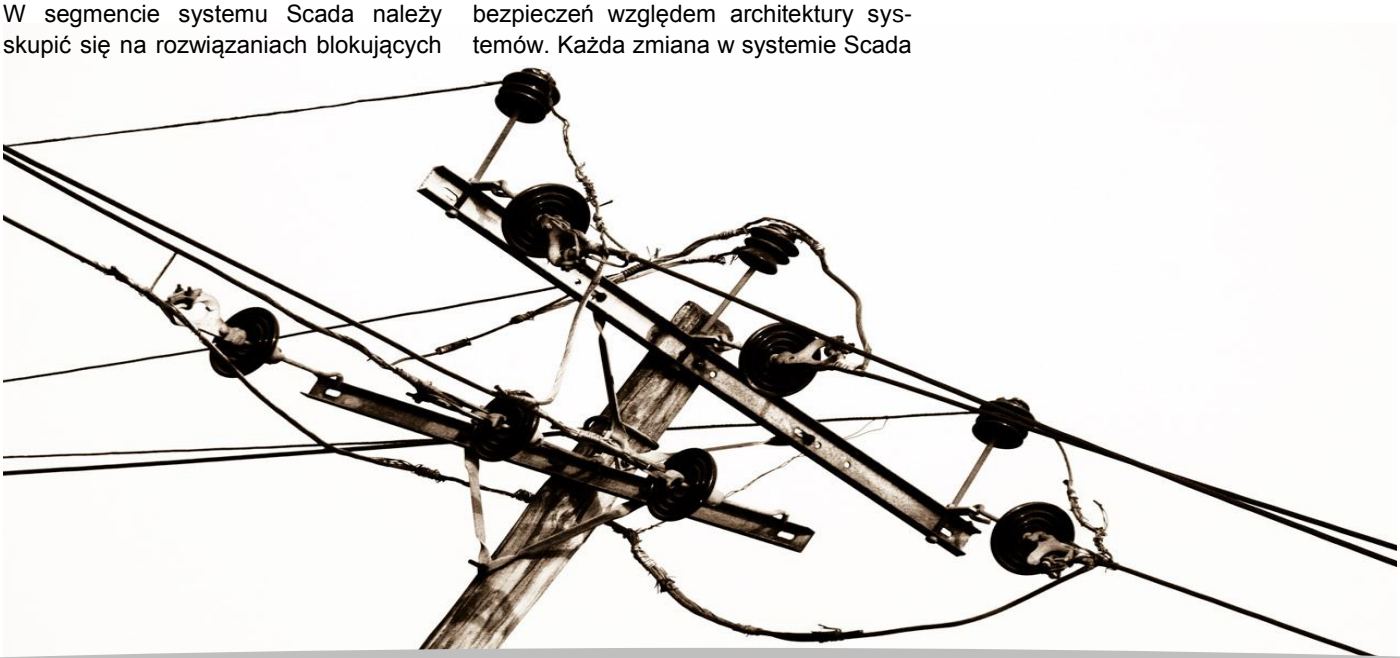
kacyjną węzła wymiany danych pomiędzy systemem Scada a światem zewnętrznym powinien być DMZ, w którym zlokalizowane będą systemy transakcyjne, do których segment Scada będzie dostarczał dane oraz do których będzie się zwracał po autoryzowane zapytania o ich dostarczenie. Rozwiązanie to umożliwiłoby wdrożenie na styku komunikacyjnym najprostszej z możliwych reguł ochrony: zabroń jakiejkolwiek próby komunikacji z zewnątrz do systemów Scada. Systemy bezpieczeństwa powinny być zlokalizowane pomiędzy systemem Scada, a strefą DMZ, a w celu zapewnienia możliwości pełnej analizy ruchu, szyfrowanie powinno być zakończone jeszcze przed DMZ od strony sieci publicznych i pozostałych systemów przedsiębiorstwa. Ze względu na fakt, iż nie każde z obecnie stosowanych rozwiązań komunikacyjnych da się migrować do tej postaci, należy podjąć szczególne starania, by precyzyjnie zidentyfikować, jakie urządzenia i po jakie dane sięgają do systemów Scada i ograniczyć komunikację na brzegu sieci wyłącznie do tych protokołów i tych urządzeń. Włączenie zabezpieczeń wbudowanych w protokoły komunikacyjne jest kolejnym etapem podnoszenia poziomu bezpieczeństwa (jeżeli jeszcze nie zostało wykonane). Zabezpieczenia takie jak, walidacje poleceń, sprawdzanie stempli czasowych, sprawdzanie poprawności składni, raportowanie o błędach pozwolą na eliminację błędnych zapytań i poleceń, a także zwiększą prawdopodobieństwo wykrycia zagrożenia. Należy bowiem podkreślić, iż tak wdrożony DMZ będzie granicą pomiędzy światem dynamicznych zmian sieci przedsiębiorstwa i publicznej Internet, a stabilnością systemu Scada.

W segmencie systemu Scada należy skupić się na rozwiązaniach blokujących każdą nieautoryzowaną komunikację oraz wykrywających wszelkie próby łączności, jakie nie zostały wcześniej zatwierdzone. Mając dokumentację systemu można bowiem określić precyzyjnie, które serwery i aplikacje będą się pomiędzy sobą komunikować oraz jakie to będą protokoły. Określenie, do których systemów będą kierowane zapytania bazodanowe, do których webowe, a które systemy będą wysyłały pakiety IEC104 lub ICCP, dla administratora posiadającego pełnię wiedzy o systemie Scada nie powinno nastręczać jakichkolwiek trudności. Z dużym prawdopodobieństwem należy założyć, iż tak szczegółowej wiedzy nie będzie posiadał ani napastnik, ani tym bardziej popularne złośliwe oprogramowanie, które może przedostać się przypadkiem do segmentu sieci systemu Scada. Wdrożenie zabezpieczeń na poziomie serwerów, a jeszcze lepiej w segmencie centralnym sieci Scada, pozwoli na wykrycie anomalii lub ataku w fazie rozpoznawania przez napastnika systemu. Zabezpieczeniem najwyższego rzędu, wspierające pracę administratorów odpowiedzialnych za bezpieczeństwo, mogą być systemy klasy SIEM, które zbiorą i zanalizują dane o bezpieczeństwie zgromadzone przez zabezpieczenia na styku z DMZ oraz w segmencie Scada.

Powyższą architekturę należy budować zarówno dla systemu Scada centralnego nadzoru, jak i dla systemów w lokalizacjach zdalnych. Istotnym elementem jest, by odpowiednio do potrzeb bezpieczeństwa dostosować procesy eksploatacyjne infrastruktury, w szczególności związane z rozwojem i modernizacją systemów technologicznych oraz systemów Scada tak, by zapewnić ciągłą aktualność zabezpieczeń względem architektury systemów. Każda zmiana w systemie Scada (dodanie nowego urządzenia PLC lub protokołu komunikacyjnego) powinna być modelowana również w systemie bezpieczeństwa.

Wdrażanie powyżej opisanych zabezpieczeń nie powinno nieść za sobą nadmiernych kosztów, główny ich ciężar bowiem wynika z pracochłonności wymaganej do poznania i zamodelowania pracy systemu Scada, znajomość własnych systemów zwraca się jednak po stokroć, jeśli przełożymy ją na wpływ na bezawaryjność ich pracy. Systemy detekcji anomalii dostępne są w wydaniu Open Source (darmowe dla przedsiębiorstw), a ich wymagania sprzętowe spełni każdy z wycofywanych z eksploatacji komputerów. Budowa scentralizowanego węzła komunikacyjnego DMZ powinna wpłynąć na obniżenie kosztów związanych z zapewnieniem wymiany danych przez Scadę ze światem systemów zewnętrznych, nie będzie już bowiem występowało mnożenie się pojedynczych kanałów oraz zabezpieczeń dla każdego z nich . SIEM może zostać scentralizowany, zbierać oraz analizować dane ze wszystkich systemów Scada(centralnego i zdalnych), a znajomość chronionej przez niego architektury powinna w sposób znaczny obniżyć koszty jego wdrożenia.

Tadeusz Włodarczyk, lat 34, absolwent Wyższej Szkoły Informatyki Stosowanej i Zarządzania pod auspicjami Polskiej Akademi Nauk, od 12 lat zajmuje się w PSE Operator S.A. bezpieczeństwem informacji i systemów teleinformatycznych, od roku członek grupy ekspertów ds. bezpieczeństwa sieciowego przy ENTSO-E.



Czy infrastruktura krytyczna jest rzeczywiście krytyczna?

Parę słów o bezpieczeństwie (tele)informatycznym...

Michał Kraut
Cisco Systems

Dyskusje o bezpieczeństwie infrastruktury krytycznej trwają już od dawna. I bynajmniej nikt w czasie ich trwania nie podważa znaczenia tej infrastruktury. Jednakże, kiedy spojrzymy na postęp prac, projektów, które mają na celu zwiększenie realnego bezpieczeństwa tej infrastruktury, to już okazuje się, że ilość instytucji, które mogą pochwalić się znaczącymi sukcesami, nie jest taka duża jak liczba zabierających głos w dyskusji. Dzieje się tak, pomimo tego, że dostępne są dokumenty i rekomendacje pokazujące, jak można wykonać pierwsze kroki w celu podniesienia poziomu bezpieczeństwa, a wielu producentów oferuje stosowne rozwiązania. Czy zatem krytyczność infrastruktury (ta rzeczywista i ta „postrzegana") idzie w parze z konkretnymi działaniami, a jeśli już, to czy te działania mają równie wysoki, lub nawet „krytyczny" priorytet ?

Ochrona teleinformatyczna infrastruktury krytycznej to jedna z najszybciej rozwijających się dziedzin. Wynika to między innymi z procesu wprowadzania protokołu IP do środowisk przemysłowych. Objawia się to możliwością budowy systemów komunikacyjnych dla zarządzania produkcją (DCS, SCADA) w oparciu o typowe rozwiązania sieciowe. Pozwala to skorzystać z dorobku wielu lat doświadczeń w budowaniu systemów sieci komputerowych, ale pociąga to też za sobą określone konsekwencje związane z bezpieczeństwem. Dalej za tym podążają rekomendacje i architektury referencyjne dla budowy poszczególnych systemów proponowane przez producentów rozwiązań. Niestety w pierwszych wersjach dokumenty te tworzone były często bez uwzględnienia specyfiki dwóch światów jakimi były silosowe rozwiązania przemysłowe w przeszłości i otwarty świat komunikacji IP. Skutkowało to nieraz bardzo rygorystycznymi architekturami dla nowych systemów komunikacyjnych obsługujących rozwiązania ICS (Industrial Control), których parametry zniechęcały do wdrożeń, szczególnie w dynamicznym środowisku IP. Ostatecznie powodowało to bądź dowolność i częstą zmienność interpretacji, bądź wnioskowanie, że budowa systemów bezpieczeństwa jest niemożliwa ze względu na zbyt wygórowane wymagania. Obecnie coraz więcej rekomendacji jest zorientowana na zapewnienie ciągłości działania infrastruktury krytycznej, nie definiując wszędzie sztywnych wymagań, a jedynie parametry niezawodnościowe i określając wpływ braku poprawnego działania danego elementu systemu na jego całość i to w określonym oknie czasowym. Takie podejście oczywiście w żaden sposób nie zmienia ilości i rodzaju zagrożeń dla infrastruktury, nie zmienia też zakresu wymagań (należy pamiętać, że w części rekomendacji pojawiają się też wymagania „miękkie" jak szkolenie pracowników, sposoby informowania o zagrożeniach zauważonych przez pracowników etc). Zmienia się jednak na tyle dużo, że architekci systemów bezpieczeństwa mogą zaproponować szereg różnych rozwiązań technologicznych pozwalających na uzyskanie pożądanych parametrów sprawności systemu infrastruktury krytycznej.

Skoro zatem nowe standardy i rekomendacje będą dawały większą swobodę realizacji systemu zabezpieczeń warto się przyjrzeć ich szkicom lub ostatecznym wersjom oraz podjąć wysiłek ich przełożenia, lub inaczej - zamapowania na własną organizację. To mapowanie będzie musiało odbyć się wielowymiarowo co wynika z kilku perspektyw, z których możemy spojrzeć na kwestie bezpieczeństwa infrastruktury.

Pierwsza z nich to kwestia przepływu informacji w organizacji – czyli opis tego jak komunikują się poszczególne jednostki organizacyjne w firmie lub w grupie kapitałowej. Jak przebiega komunikacja pomiędzy obiektami (technicznymi, biurowymi) w różnych lokalizacjach. Które aplikacje muszą się ze sobą komunikować bezpośrednio, które współdzielą dane, które komunikacji nie potrzebują. Dodatkowym utrudnieniem jest to ,że należy to zrobić zarówno dla aplikacji stricte związanych z działalnością firmy (np. SCADA) jak aplikacji wspomagających. To mapowanie wymagań ochrony na procesy i przepływ informacji w firmie pozwoli na uporządkowanie lub usystematyzowanie strumieni komunikacyjnych, pozwoli też dobrać odpowiednie narzędzia wymuszające politykę wymiany informacji.

Inną perspektywą jest zamapowanie wymagań na architekturę systemu przemysłowego, w szczególności na to, jak zbudowana jest tzw. strefa kontrolna oraz strefy „podległe". Ważnym aspektem jest określenie krytyczności poszczególnych obszarów, zwrócenie uwagi na elementy ochrony kontrolerów PLC, napędów, sensorów, systemów zarządzania. I to zarówno od strony ich samych jako urządzeń działajacych w

przemysłowym środowisku IP, jak też od strony lokalnego czy zdalnego dostępu do tych urządzeń np. dla inżynierów, którzy realizują kontrakty serwisowe producenta danego systemu. Należy też określić, w jaki sposób strefa kontrolna jest lub ma być skomunikowana z siecią administracyjną – i tu już wracamy do poprzednio omówionego zagadnienia, ale też wskazujemy następne, czyli kontrolę dostępu.

Większość architektur referencyjnych podnosi to jako jeden z kluczowych elementów. Oczywistym jest, że poszczególne systemy muszą się ze sobą komunikować – w sposób kontrolowany i uporządkowany. Jednakże dostęp z sekretariatu zarządu do systemów zarządzania stacją energetyczną niekoniecznie jest pożądany. I nie można tutaj poprzestać na „umownych" ustaleniach określających rozdział systemów ICS od systemów administracyjnych. Poszczególne narzędzia realizujące wskazane zadania ochrony muszą posiadać możliwość wymuszenia praw dostępu dla poszczególnych użytkowników czy grup użytkowników do wskazanych zasobów. Czyli niejako przełożyć silne wymagania wskazane przez administratorów bezpieczeństwa na rozwiązania techniczne. Silne wymagania określają tutaj jasną i przejrzystą politykę dostępu do zasobów – np. systemu DCS – jako wskazanie nie tylko osoby, która może uzyskać dostęp, ale też urządzeń, z których ten dostęp będzie możliwy i miejsca (np. niedopuszczalne jest żeby uprawniony pracownik dokonywał zmian w systemach zarządzania infrastrukturą krytyczną korzystając z prywatnego laptopa lub tabletu, lub np. uzyska ograniczony dostęp jeżeli będzie pracował zdalnie przez VPN). Politykę kontroli dostępu również należy tworzyć całościowo - tak dla systemów przemysłowych jak i administracyjnych. W wielu przypadkach tak skonkretyzowane i „silne" wymagania dotyczące dostępu do zasobów są specyzowane dla systemów przemysłowych, jednak zwykle nie są one zdefiniowane dla systemów administracyjnych. Stawiając jednak pytanie „po co to robić ?" należy wziąć pod uwagę aspekt pierwszy – przepływ informacji. Jeżeli będzie się on w jakikolwiek sposób odbywał pomiędzy siecią administracyjną i przemysłową, to znaczy, że należy go kontrolować. Zatem ta perspektywa jest trochę mniej techniczna, bardziej organizacyjna i administracyjna, ale co ciekawe i ważne dotyka jeszcze innej perspektywy... mapowania wymagań na dostępne rozwiązania techniczne.

Ta ostatnia perspektywa poruszana w tym opracowaniu ma na celu zweryfikowanie czy pożądany poziom bezpieczeństwa (opisany wymaganiami) jest możliwy do uzyskania z wykorzystaniem dostępnych rozwiązań oferowanych przez producentów. Dotyczy to bardzo szerokiego spektrum zastosowań – od rozwiązań realizujących stricte funkcje zabezpieczenia informacji poprzez rozwiązania bezpieczeństwa fizycznego i monitoringu wizyjnego, a skończywszy na systemach zarządzania, raportowania i monitoringu zdarzeń w systemach informatycznych. To mapowanie wymagań na technologię może być największym wyzwaniem – ze względu na ilość pojawiających się nowych rozwiązań i rozszerzanie funkcjonalności produktów już dostępnych. Może okazać się, że analiza przygotowana przed trzema miesiącami będzie już nieaktualna. To jednak jest tylko czynnikiem sprzyjającym uzyskiwaniu wyższego poziomu bezpieczeństwa infrastruktury krytycznej – mamy do dyspozycji coraz więcej ,coraz lepszych rozwiązań.

Dochodzimy zatem do pewnego istotnego wniosku, którym jest stwierdzenie dostępności szeregu rozwiązań i modeli architektur, których zastosowanie może podnieść poziom bezpieczeństwa infrastruktury krytycznej. Oczywiście żadna z nich nie jest na dziś architekturą kompletną, adresującą wszystkie możliwe zagrożenia i wszystkie możliwe scenariusze wdrożeniowe dla systemów teleinformatycznych w infrastrukturze krytycznej, jednakże pewne obszary zostały ja-

sno i konkretnie zdefiniowane i do nich z pewnością warto się odnieść. Te obszary to przede wszystkim:

● Odseparowanie sieci ICS od sieci administracyjnej. Pozwala to na wprowadzenie tzw. elementów bezpieczeństwa brzegu sieci w tym ścian ogniowych (*firewall*) i systemów zapobiegania włamaniom (*IPS*). Taki ruch ochroni sieć ICS przed wirusami i anomaliami, które mogą wystąpić w sieci administracyjnej, pomoże ochronić sieć ICS przed dostępem do niej z dowolnego innego miejsca w sieci administracyjnej oraz pozwoli w sposób przejrzysty kontrolować do niej dostęp.

● Organizacja bezpieczenego dostępu do sieci ICS tak, aby z jednej strony kontrolować ten dostęp zarówno dla pracowników organizacji jak też kooperantów/dostawców wykonujących usługi serwisowe. Dotyczy to m.in. wydzielenia określonych stref, do których mają dostęp poszczególne osoby i zminimalizowanie ryzyka związanego z nadużyciami (np. poprzez separację środowisk poszczególnych dostawców). Model ten może dotyczyć tylko sieci lokalnej, ale także zdalnego dostępu. Zbudowanie modelu kontroli dostępu umożliwi jednoznaczne określenie warunków, w których pracownik lub dostawca będzie mógł pracować na systemach ICS dla infrastruktury krytycznej – uwierzytelnienie osoby, uwierzytelnienie urządzenia (komputera), czas, sposób dostępu (lokalny czy zdalny), systemy zabezpieczeń na stacji, która będzie wykorzystywana do pracy (np. aktualny system antywirusowy) etc. Ponadto wypracowanie modelu dostępu (również zdalnego) pozwoli na jego „standaryzację" – we wszystkich obiektach należących do organizacji zarządzającej infrastrukturą krytyczną

● Budowa modelu komunikacyjnego dla stacji energetycznej, w którym następuje rozdzielenie sieci dla systemów witalnych dla stacji (telemechanika, opomiarowanie etc.) od systemów wspomagających (sieć wielousługowa), w której mogą znaleźć się takie usługi jak wideomonitoring, telefonia IP, dostęp do sieci administracyjnej oraz sieć powiązana ze SmartMetering. Na dziś bezdyskusyjnym jest rozdział tych dwóch obszarów – jest to rekomendowane w wielu architekturach referencyjnych. Oczywiście niektóre architektury posuwają się dalej i wskazują na konieczność umieszczenia poszczególnych systemów z sieci wielousługowej w wydzielonych logicznie sieciach per usługa. Nie zmienia to jednak faktu dostępności gotowych modeli dla wdrożenia sieci w obiektach technicznych infrastruktury krytycznej. Sposób segmentacji sieci i jej granularność leży w gestii architekta rozwiązania, który poza uzyskaniem wyższego poziomu bezpieczeństwa i przygotowania wskazań dla ustandaryzowania konfiguracji może też przyczynić się rozwoju SmartGrid.

● Budowa bezpiecznej platformy komunikacyjnej dla przedsiębiorstwa zarządzającego infrastrukturą krytyczną. Mówimy tutaj o podobnym modelu jak w przypadku sieci dla obietów technicznych, ale w odniesieniu do całości przedsiębiorstwa – wykorzystania pojedynczej infrastruktury fizycznej (urządzenia komunikacyjne) do stworzenia wielu sieci wirtualnych i odseparowania komunikacji z systemów SCADA, transmisji głosowej, transmisji wideomonitoringu, sieci administracyjnej i innych od siebie wzajemnie. W takim modelu każda z nich może być osobno zarządzana, każda może mieć indywidualne parametry dostosowane do specyfiki transmisji. Jednocześnie dzięki wirtualizacji możliwe jest obniżenie kosztów całości inwestycji. Powyższa lista z pewnością nie wyczerpuje wszystkich dostępnych rozwiązań. Jest ich zdecydowanie więcej, a jednym z najważniejszych obecnie zadań dla koordynatorów bezpieczeństwa infrastruktury krytycznej jest wypracowanie na ich bazie fundamentów dla architektury bezpieczeństwa dla tej infastruktury. Rzetelny przegląd rozwiązań powinnien pozwolić na wstępny ich wybór i „logiczne" umieszczenie w aktualnej strukturze i o ile ogólność wymagań może powodować rozbieżności interpretacyjne, to z pewnością nie będzie to dotyczyło pryncypiów. Architektura ta musi być też otwarta na „nowe" – tak rozwiązania, jak i wymagania, tak by budując fundamenty móc z nich korzystać przy rozbudowie systemów ochrony.

I na koniec warto też dodać, że w przypadku bezpieczeństwa dążenie do ideału będzie dążeniem do kolejnej „dziewiątki" w 99,(9)% - w przypadku ochrony teleinformatycznej infrastruktury krytycznej prawie każda inicjatywa będzie nas do tego przybliżać. A każde rozwiązanie punktowe będzie dobre o ile będzie się wpisywać w całościową architekturę.

Michał Kraut - o*dpowiada za rozwój sprzedaży produktów bezpieczeństwa. Od wielu lat związany z rynkiem produktów bezpieczeństwa. Poprzednio w firmach integratorów IT oraz operatorów telekomunikacyjnych. W latach 2000-2008 pełnił rolę doradczą dla działu rozwoju produktów bezpieczeństwa Cisco, a od 2009 zaangażowany jest w podobnej roli dla działu SmartGrid. Związany z projektami dla sektora paliwowego, energetycznego oraz w sektorze publicznym - głównie w zakresie rozwiązań sieciowych i bezpieczeństwa teleinformatycznego.*

System zarządzania procesami bezpieczeństwa w administracji państwowej RP

Przemysław Frasunek

ATM Systemy Informatyczne SA

Bezpieczeństwo demokratycznego państwa zależy dzisiaj w dużej mierze od gotowości administracji publicznej i wojska do reagowania na incydenty zagrażające integralności cyberprzestrzeni kraju i bezpieczeństwu informacji.

W ostatnich latach miało miejsce szereg wydarzeń, które pokazały, jak bardzo istotne jest skuteczne zarządzanie incydentami i bezpieczeństwem systemów teleinformatycznych. Przytoczyć tu można przykłady takie jak:

- cyberataki na infrastrukturę rządową Estonii w 2007 r.,
- cyberataki prowadzone przez obydwie strony konfliktu zbrojnego w Osetii Południowej w 2008 r.,
- cyberataki na polską infrastrukturę rządową w trakcie protestów przeciwko podpisaniu umowy ACTA w 2012 r.,
- ataki mające na celu sabotowanie irańskiego programu nuklearnego i wykorzystujące zaawansowane oprogramowanie szkodliwe: Stuxnet (2010 r.), Duqu (2011 r.), Flame (2012 r.).

Zapewnienie odpowiedniego poziomu bezpieczeństwa informacji narzuca na administrację publiczną konieczność ciągłego podnoszenia poziomu wiedzy, szybkiej identyfikacji zagrożeń, analizowania incydentów i wdrażania odpowiednich metod w celu zminimalizowania na przyszłość podatności systemów. Aby spełnienie tych wymagań było możliwe, konieczne jest posiadanie odpowiednich narzędzi informatycznych, które automatyzują wybrane procesy związane z zarządzaniem bezpieczeństwem IT.

HISTORIA I ZAŁOŻENIA PROJEKTU

W 2011 r. Narodowe Centrum Badań i Rozwoju opublikowało założenia do konkursu z zakresu obronności i bezpieczeństwa państwa. Jednym z zadań konkursowych było opracowanie i zbudowanie systemu zarządzania bezpieczeństwem teleinformatycznym jednostek Resortu Obrony Narodowej, wraz z narzędziami wspomagającymi zwalczanie zagrożeń i ochronę teleinformatycznej infrastruktury krytycznej.

Konkurs ten został rozstrzygnięty pod koniec 2011 r., a realizacja projektu została powierzona konsorcjum złożonemu z firm ATM Systemy Informatyczne S.A. oraz NASK. Zaplanowany okres realizacji projektu to lata 2012-2013.

We wniosku konkursowym konsorcjum zaproponowało stworzenie w pełni funkcjonalnego i rozproszonego Systemu Bezpieczeństwa Teleinformatycznego, obejmującego trzy obszary zastosowań:

- zarządzanie cyklem życia systemów teleinformatycznych oraz ewidencją sprzętu i oprogramowania eksploatowanego w resorcie,
- zarządzanie bazą podatności i zagrożeń w oprogramowaniu, zawierającą testy, pozwalające na automatyczne określenie listy zagrożonych systemów teleinformatycznych,
- zarządzanie przepływem pracy przy obsłudze incydentów komputerowych i certyfikacji projektów, systemów i urządzeń.

Obsługa incydentów jest jednym z priorytetów SBT. Dotychczas nie został wdrożony w kraju żaden wspólny system obsługi incydentów, który pozwoliłby na scentralizowane zarządzanie i korelowanie incydentów zgłaszanych przez różne organy administracji publicznej. Systemy i procedury związane z obsługą incydentów są utrzymywane niezależnie przez zespoły CERT GOV, CERT NASK, SRnIK MON (MIL CERT) oraz operatorów telekomunikacyjnych (TPSA, Pionier, …), przy czym są one zazwyczaj niekompatybilne, a wymiana wiedzy pomiędzy tymi zespołami odbywa się drogami tradycyjnymi.

Prowadzone w styczniu 2012 r. ataki typu DDoS skierowane przeciwko systemom teleinformatycznym administracji publicznej RP wykazały, że efektywna wymiana informacji o charakterystyce ataków, ich celach oraz adresach źródłowych napastników mogłaby pozwolić na ograniczenie niedostępności atakowanych systemów.

Ideą podsystemu obsługi incydentów w SBT jest agregowanie ustrukturalizowanych informacji o incydentach bezpieczeństwa odnotowanych w sieciach resortowych. Informacje takie, w przypadku wyrażenia woli przez administratora będą propagowane do wybranych, zewnętrznych zespołów CERT, przy użyciu interfejsów automatycznych. Taki przebieg komunikacji wykorzystywany będzie w sytuacji, gdy incydent dotknie nadzorowanych systemów, natomiast jego źródłem będą systemy lub użytkownicy będące w jurysdykcji innego zespołu CERT.

W SBT założono także implementację interfejsów przyjmujących informacje o incydentach z zewnętrznych źródeł. Interfejsy te będą udostępniane w sposób bezpieczny zaufanym zespołom CERT. Pozwolą one na raportowanie incydentów, których źródłem są systemy nadzorowane przez SBT.

Ponadto, zakłada się, że również zewnętrzne wobec SBT systemy eksploatowane w resorcie mogą być źródłem informacji o incydentach. Przykładem takich źródeł mogą być: systemy IDS/IPS, oprogramowanie antywirusowe, czy sondy systemu ARAKIS-GOV.

SFORMALIZOWANA REPREZENTACJA DANYCH

Jednym z istotnych założeń proponowanego systemu jest wykorzystanie standardów z rodziny SCAP (*Security Content Automation Protocol*) rozwijanych przez NIST (USA) do sformalizowanego, jednolitego opisu różnych aspektów bezpieczeństwa systemów - polityki bezpieczeństwa, konfiguracji, podatności, zagrożeń, incydentów listy oprogramowania złośliwego oraz reguł automatycznych testów. Zgodność projektowanego systemu z powyższymi standardami pozwoli na wykorzystanie istniejących źródeł danych i na efektywną wymianę informacji z sojuszniczymi systemami do zarządzania bezpieczeństwem teleinformatycznym.

Obecna wersja standardu SCAP posiada numer 1.2 i została wydana we wrześniu 2011 roku, w publikacji NIST o numerze SP800-126r2. W skład standardu wchodzi 11 specyfikacji poszczególnych modułów:

● Języki – pozwalają na sformalizowaną reprezentację polityk bezpieczeństwa, mechanizmów testów bezpieczeństwa oraz wyników tych testów:

○ OVAL (*Open Vulnerability and Assessment Language*) 5.10 – standard określający format danych bazujący na XML i służący opisywaniu podatności oraz błędów w oprogramowaniu, testów ich występowania i sposobów zapobiegania, oraz raportowaniu o nich,

○ XCCDF (*Extensible Configuration Checklist Description Format*) 1.2 – standard określający sposób wyrażania wymagań co do systemu i raportowania wyników oceny zgodności w języku XML,

○ OCIL (*Open Checklist Interactive Language*) 2.0 – standard opisu kwestionariuszy, pozwalających na manualną ewaluację zgodności z polityką bezpieczeństwa,

●Formaty raportów – pozwalają na sformalizowane wyrażanie informacji przetworzonych przez systemy zarządzające procesami bezpieczeństwa:

○ ARF (*Asset Reporting Format*) 1.1 – model danych opisujący złożone systemy, ich komponenty oraz związki pomiędzy komponentami, enkapsulujący (hermetyzujący) raporty w formacie OVAL i XCCDF,

○ AI (*Asset Identification*) 1.1 – model danych, pozwalający na jednoznaczne identyfikowanie i sklasyfikowanie systemów teleinformatycznych,

● Nazewnictwo, słowniki – określają standardowy format nazw i słownik artefaktów związanych z bezpieczeństwem teleinformatycznym:

○ CPE (*Common Platform Enumeration*) 2.3 – słownik identyfikatorów platform sprzętowych i programowych,

○ CCE (*Common Configuration Enumeration*) 5 – słownik zmiennych konfiguracyjnych, mających wpływ na bezpieczeństwo systemu,

○ CVE (*Common Vulnerabilities and Exposures*) – słownik identyfikatorów podatności związanych z wykorzystaniem konkretnych słabości oprogramowania,

● Skale i mechanizmy porównawcze – opisują sposób ewaluacji cech charakterystycznych poszczególnych podatności i słabości konfiguracyjnych, prowadzący do wystawienia relatywnej oceny ryzyka dla zagrożonych systemów teleinformatycznych:

○ CVSS (*Common Vulnerability Scoring System*) 2.0 – standard definiujący zasady oceny ważności zagrożeń wynikających z podatności sprzętu i oprogramowania,

○ CCSS (*Common Configuration Scoring System*) 2.0 – standard definiujący zasady oceny ważności zagrożeń wynikających ze słabości konfiguracyjnych,

● Integralność – opisuje mechanizmy zabezpieczenia integralności danych wyrażonych zgodnie z wyżej opisanymi notacjami:

○TMSAD (*Trust Model for Security Automation Data*) 1.0 – standard kryptograficznego zabezpieczania dokumentów XML z wykorzystaniem specyfikacji XMLDSIG.

Standardy SCAP są aktywnie promowane przez rząd USA, zostały także zaimplementowane w szeregu komercyjnych produktach wspierających bezpieczeństwo teleinformatyczne.

ARCHITEKTURA SYSTEMU

Autorzy koncepcji zaproponowali podział projektowanego systemu na trzy zasadnicze moduły:

System Zarządzania Procesami Bezpieczeństwa (SZPB)

SZPB jest aplikacją typu *workflow management*, która zapewnia odpowiedni przebieg procesów projektowania, certyfikacji, wdrażania, eksploatacji i wycofywania oraz efektywne współdziałanie wielu jednostek organizacyjnych.

Celem systemu jest wspieranie procesów zarządczych, określonych na etapie analizy i zapisanych w notacji BPMN/BPML. SZPB stanowi centralny element systemu, do którego przekazywane są zagregowane i przetworzone informacje na temat stanu poszczególnych nadzorowanych systemów i działań podejmowanych przez osoby odpowiedzialne za ich bezpieczeństwo.

SZPB gromadzi dane o systemach teleinformatycznych, zawiera bazę certyfikowanych komponentów wraz z opisem polityk bezpieczeństwa i komunikuje się z systemami sojuszniczymi w celu aktualizacji bazy zagrożeń.

Edytor Bezpieczeństwa STI (EB)

EB jest narzędziem wspierającym proces projektowania systemów teleinformatycznych poprzez wizualizację biblioteki akredytowanych komponentów oraz bieżące badania zgodności stanu komponentów systemów teleinformatycznych z polityką bezpieczeństwa, wyrażoną przy pomocy notacji XCCDF (SCAP). EB pełni również funkcję narzędzia wspierającego tworzenie polityk bezpieczeństwa XCCDF i testów OVAL.

Agent do Testów OVAL (ATO)

Rolą ATO jest analiza zgodności stanu wybranego systemu teleinformatycznego z założoną polityką bezpieczeństwa, zdefiniowaną przy pomocy XCCDF w SZPB oraz określanie listy zagrożonych systemów na podstawie informacji o podatności. Agent bada zgodność, wykonując zestaw testów, opisanych w języku OVAL. Niektóre z testów mogą polegać na komunikacji z innymi aplikacjami np. z programem antywirusowym, lokalnym systemem firewall, bądź narzędziami służącymi do przeprowadzania testów penetracyjnych.

STAN REALIZACJI PROJEKTU I PLANY NA PRZYSZŁOŚĆ

Z końcem sierpnia 2012 r. w projekcie zakończono prace analityczne i rozpoczęto prace projektowe oraz implementacyjne. Zakończenie projektu i wdrożenie pilotażowe jest planowane na koniec 2013 r. Zdaniem autorów systemu, po wdrożeniu ma on potencjał do objęcia funkcji narodowej bazy podatności, na wzór bazy NVD utrzymywanej przez NIST oraz systemu zarządzającego obsługą i wymianą danych o incydentach informatycznych, dotykających infrastruktury rządowej.

Przemysław Frasunek jest dyrektorem ds. rozwoju produktów w Centrum Badawczo-Rozwojowym ATM-Lab sp. z o.o., spółce z grupy kapitałowej ATM S.A. odpowiedzialnej za opracowywanie nowych produktów i usług.

Następny numer „CIIP focus" ukaże się pod koniec listopada.
Zachęcamy do kontaktu z redakcją "CIIP focus"