Sektor energetyczny i cyberbezpieczeństwo

Autor: prof. dr hab. inż. Jacek Malko, dr inż. Henryk Wojciechowski, Instytut Energoelektryki, Politechnika Wrocławska

("Nowa Energia" - nr 1/2015)

Rosnące ryzyko cyberataków na sektor dostaw energii stwarza dla operatorów systemów informatycznych infrastruktury energetycznej zagrożenie, którego nie sposób zlekceważyć. Problem cyberbezpieczeństwa w energetyce stał się „tematem okładkowym" *(„cover-story")* wydania specjalnego magazynu firmy medialnej PennWell - Power Engineering International z października 2014 r. [1] (rys. 1).

Rys. 1. Fragment z okładki magazynu PEI Power Engineering International z października 2014 r.

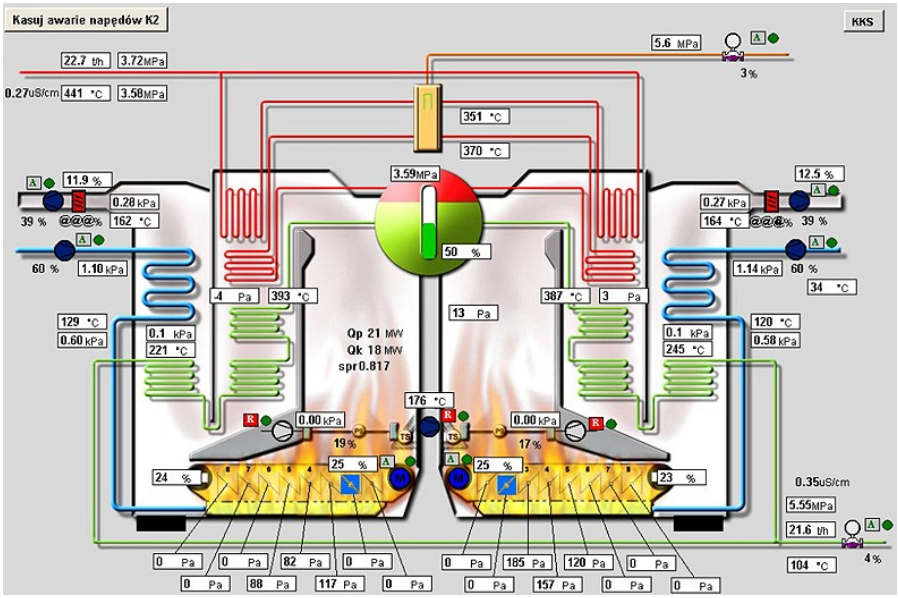
Usytuowanie Polski na geopolitycznej mapie świata i realia podjętego przez polską politykę zagraniczną różnorodnego angażowania się w globalną walkę z terroryzmem skłaniają do przyjrzenia się sytuacji, opisywanej przez analityka PEI w formie poradnika ochrony przedsiębiorstw energetycznych, wykorzystującego i komentującego opinie wielu światowych ekspertów w tej dziedzinie.

Nieprzerwanie napływają doniesienia o nowych czynnikach ryzyka dla operatorskiego zarządzania infrastrukturą energetyki. Niektóre z tych czynników ujawniły się dopiero niedawno, a wieści o nich wybiły się na czołówki doniesień jako działania podjęte w złej wierze i przypisywane podmiotowi o łatwym do rozszyfrowania kryptonimie „Energetyczny Niedźwiedź" *(„Energy Bear")*. Również powtarzalne ataki na południowokoreańskie elektrownie jądrowe w grudniu 2014 r. jednoznacznie kojarzono z „braćmi z północy". Ryzyko cyberataków stale rośnie. Raport opublikowany przez analityków firmy Kaspersky Lab.

(zajmującej się bezpieczeństwem sieci komputerowych) donosi, że 91% firm wykryło w 2013 r. ataki na swoje systemy. Eksperci z branży komputerowej stwierdzili, że pozostające w cieniu Energy Bear grupy hakerskie (działającepod zbiorczym pseudonimem „Ważka" - *„Dragonfly"*) zintensyfikowały w ostatnich miesiącach ataki na software'owe zabezpieczenia. Do marca 2014 r. wykryto cybergrupy przestępcze, zainteresowane działaniami dywersyjnymi, 50% z nich skupiało się na sektorze energetycznym, zaś 30% - na systemach sterowania w energetyce. W lipcowym (2014) raporcie firma Symantec opisała zakrojoną szeroko operację grupy Dragonfly w zakresie ataków na firmy sektora energii w USA, Hiszpanii, Francji, Włoszech, Niemczech, Turcji i Polsce (!). Celem tych ataków byli operatorzy sieci elektroenergetycznych, wielkie przedsiębiorstwa wytwórcze, operatorzy rurociągów naftowych oraz dostawcy urządzeń. Raport stwierdza, iż zorganizowane grupy hakerów wykorzystywały nielegalny dostęp do tych podmiotów jako narzędzia szpiegowania, ale możliwości działań stricte sabotażowych są realne i mogą prowadzić do zakłócenia lub przerwania dostaw energii w wielu krajach. Istnieje zatem istotna wrażliwość infrastruktury energetycznej. Jak zatem możemy uchronić nasze przedsiębiorstwa przed ryzykiem związanym ze zjawiskiem cyberhakerstwa?

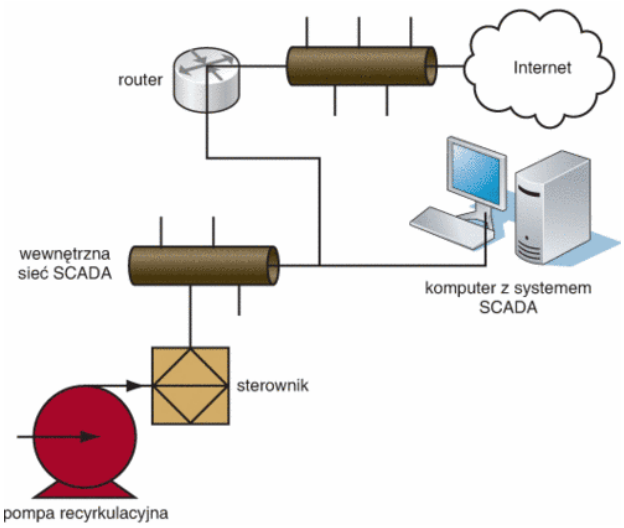
Bezpieczeństwo systemów SCADA

Ataki Dragonfly koncentrują się głównie na przemysłowych systemach sterowania. Opinie ekspertów są w tej materii wyjątkowo zgodne: najbardziej wrażliwymi w podsektorze wytwarzania energii elektrycznej są systemy SCADA (Supervisory Control and Data Acquisition). Większość z nich wykorzystuje oprogramowanie interface'owe człowiek - maszyna (HMI), umożliwiające użytkownikowi współpracę (łącznie ze sterowaniem) z urządzeniami i wyposażeniem elektrowni. Gdy haker uzyska dostęp do software'u sterującego, to jest to równoznaczne z całkowitą transparentnością oprogramowania. Systemy SCADA są obecnie szeroko rozpowszechnione w nowoczesnych technologiach przemysłowych, szczególnie w sektorze elektroenergetyki (rys. 2).



Rys. 2. Wizualizacja i sterowanie pracą kotła parowego

Wrażliwość na cyberataki wynika z oczywistego względu: architektura SCADA została opracowana zanim cyberataki stały się problemem. Wielkie elektrownie i dostawcy energii są istotnie i głęboko zagrożone, gdyż systemy te zostały wprowadzone do ówcześnie istniejących infrastruktur dekady temu i są niezabezpieczone przed cyberatakami (rys. 3).



Rys. 3. Układ przesyłu informacji niezabezpieczony przed cyberatakami

Narzędzia monitorowania, stosowane w systemach SCADA, są pomocne w integrowaniu sieci (o ile jest to możliwe - wraz z ich optymalizowaniem). W ubiegłych (15-20) latach znaczna część infrastruktury sieciowej została zbudowana w celu optymalizacji tak ukierunkowanych systemów SCADA, ale nie oczekiwano atakowania tych systemów. Mieliśmy bowiem do czynienia z realiami całkowicie odmiennymi od dzisiejszych.

Nowy partner: Microsoft

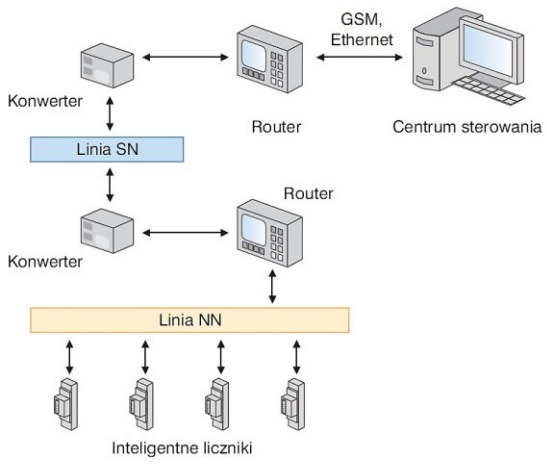
W przeszłości informatyczne systemy sterowania (ICS) funkcjonowały w pełnej izolacji od otoczenia. Nie wykorzystywano technologii IC w architekturze budowy sieci, a nawet nie opierano się na softwarze Windows jako systemie operacyjnym (OS). Nie występował zatem problem usieciowionych struktur i mikrosterowników, wbudowanych w system. Jednak gdy luka pomiędzy tymi technologiami zaczęła się zmniejszać, użytkownicy rozpoczęli domagać się struktur bardziej przyjaznych i możliwości rekonfiguracji wyposażenia. Takie wymagania są obecnie oczywistością. Przejście od systemów, opracowanych przez użytkowników do systemu operacyjnego Windows następowało stopniowo, w przedziale czasowym 1995-1999 do 2000-2001wraz z rozpowszechnieniem systemu operacyjnego XP. We wcześniejszych wersjach nie przewidziano konieczności stosowania dla bezpieczeństwa układów Windows Firewall. Od 2002 r. systemy operacyjne stały się dostatecznie wyrafinowane dla stosowania w systemach sterowania, co spowodowało ich powszechne wprowadzenie.

Jednak w 2010 r. przemysł ICS przeżył zasadniczy wstrząs, wraz z pojawieniem się wirusa Stuxnet, który zainfekował przeszło 50% komputerów w Iranie i poraził 20% instalacji jądrowych w tym kraju. Tak więc wszyscy mogli się przekonać o skuteczności działań

dywersyjnych, wymierzonych w przemysłowe systemy sterowania oraz o ich wrażliwości na bardziej masowy atak. Cyberataki grup w rodzaju Energetycznego Niedźwiedzia prowadzą do uszkodzenia obiektów, bowiem hakerzy wnikają w infrastrukturę sterowania (np. elektrowni). Może to doprowadzić do całkowitego wyłączenia, załączenia zabronionego i wszelkich innych oddziaływań. Po raz pierwszy problem okazał się aż tak poważny, gdyż w infrastrukturze krytycznej pojawili się nowi i niepożądani partnerzy. Także po raz pierwszy system dostarczania energii okazał się aż tak zagrożony w swych działaniach.

Jak hakerzy dostają się do systemu?

Wraz ze wzrastającą złożonością nowoczesnej infrastruktury energetycznej oraz rosnącą centralizacją sterowania przez systemy ICS, rośnie również związane z tym ryzyko. Zgodnie z raportem Symantech wiele systemów SCADA i ICS funkcjonuje poza tradycyjnymi ograniczeniami bezpieczeństwa i wykazuje wrażliwość na ataki hakerskie. Czasem tylko jedno kliknięcie sprowadza niebezpieczeństwo, a uchronienie się przed nim wymaga działań dalece bardziej złożonych. Istnieje internetowy adres „shodan hq.com", który jest podobny do Google'a dla systemów o dużej wrażliwości. Wejście pod ten adres i zalezienie bramek SCADA daje wskazówki odnośnie każdego zagrożenia, z nadaniem potencjalnemu użytkownikowi nazwy i hasła. Łatwo można uzyskać dostęp do zbiorczej strony (np. dla Korei Płd) i zażądać informacji np. o aktualnym poziomie mocy bloków, czy jednostkowym chwilowym zużyciu paliwa. Cyberatak staje się trywialnie prosty. Równie niebezpieczny może się okazać Metasploit, narzędzie z możliwością wykorzystania do pozyskania informacji o stanie różnych urządzeń, łącznie z monitorowaniem systemu sterowania turbin lub systemu zarządzania zbiornikami elektrowni pompowych. Na ataki narażone są wszystkie elementy, objęte powszechnym dostępem. Historia każdego ataku pozostaje w pamięci i może być wykorzystywana do ponownego użycia. Nawet początkujący haker może z tego skorzystać.



Rys. 4. Transmisja danych w inteligentnej sieci przesyłowej

Wraz z coraz powszechniejszym pojawieniem się technologii sieci inteligentnych (Smart Grids) coraz więcej nowych systemów zaopatrzenia w energię wchodzi do tzw. Internetu (rys. 4).

Rzeczy (Internet of Things), który stwarza nowy poziom wrażliwości dzięki przejrzystości dużej liczby połączonych systemów oraz niskiemu bezpieczeństwu (lub nawet jego braku), często lekceważonemu w sąsiedztwie prostych urządzeń rys. 4. Istnieje i działa ponadto „czynnik ludzki". Poza pisaniem i rozpowszechnianiem zainfekowanych programów komputerowych hakerzy używają bardziej tradycyjnych metod szpiegowania z użyciem np. wirusa zbliżonego do Stuxnet. Jednak podstawowym narzędziem jest kradzież korespondencji e-mailowej. Wystarczy do korespondencji wprowadzić niewielką fałszywą informację, a ciekawość ze strony adresata - obiektu ataku – dokona reszty. W zupełnie nieoczekiwanym punkcie można wprowadzić łącze USB i następnie zrobić z niego użytek w stacji roboczej. Gdy to nastąpi, fałszujący program rozpocznie emisję danych zgromadzonych w systemie do hakera, który kontroluje przebieg ataku swymi poleceniami i programem sterującym.

Istnieje także klasa „certyfikowanych hakerów" lub „hakerów w białych kapeluszach". W odróżnieniu od „hakerów w czarnych kapeluszach", działających w złej woli, hakerzy etyczni starają się znaleźć słabe punkty systemów, celem ich zdefiniowania i likwidacji. Idea nie polega tylko na osiągnięciu wymaganego poziomu bezpieczeństwa, ale też działaniu całościowym (holistycznym), na poziomie pakietu software'owego i wykorzystaniu fizykalnego dostępu.

Zabezpieczenie infrastruktury krytycznej

Każda opowieść o cyberbezpieczeństwie daje się streścić triadą działań „zabezpieczać, zabezpieczać i jeszcze raz zabezpieczać". Firmy działające w tym obszarze dążą do zwielokrotnienia warstw bezpieczeństwa wokół systemów krytycznych. Zabezpieczenie musi być nie tylko wielowarstwowe, ale też wielorakie, prowadząc do bezpieczeństwa w otoczeniu systemów software'owych, infrastruktury fizycznej oraz ludzkiej percepcji. Po pierwsze zarządy elektrowni muszą mieć pewność, że ich oprogramowanie jest w pełni uaktualnione i jest kompatybilne ze znanymi wrażliwościami oraz zgodnie ze standardami międzynarodowymi (np. certyfikaty SDLA). Zapewnia to, że dostawca w swych produktach zapewnia warunki cyberbezpieczeństwa i gwarantuje czas życia procesu. Wykrycie „Energetycznego Niedźwiedzia" rzuca światło na potrzebę zwrócenia uwagi na cyberbezpieczeństwo całości oprogramowania i wyposażenia zgodnie z filozofią ICS. Wymaga to upewnienia się, że zachowana została należyta staranność przy kontroli parametrów bezpieczeństwa, zapewnionych przez dostawców software-'u. Następnie musi nastąpić staranna dokumentacja wszelkich modyfikacji, powodujących zmiany w systemie zarządzania (np. elektrownią). Konieczna jest pełna informacja o historii, mogąca służyć do przewidywania cyberbezpieczeństwa na drodze wykrycia obszarów wrażliwych i dokonania uogólnień, na podstawie metody prób i błędów, przydatnej na ogół dla innych systemów i urządzeń. W celu zwiększenia bezpieczeństwa można zalecić „strefę zdemilitaryzowaną" (DMZ), zbliżoną w działaniu do technik stosowanych w armii USA. Mamy wówczas silną osłonę zewnętrzną, mocne „ściany ogniowe", których pokonanie daje dopiero dostęp do struktur pośrednich i do innych ścian ogniowych, ale mniej agresywnych w reagowaniu i umożliwiających interfejsowi człowiek – maszyna (HMI) spokojne działanie bez istotnych opóźnień. Dalej napotykamy

następną ścianę ogniową, bądź router o prostej liście kontrolnej dostępu i wreszcie znajdujemy się w centrum systemu. Wbudowane systemy są dostatecznie czułe, by czasem reagować przez wyłączenie. Konieczne jest wówczas dalsze utwardzenie warstwy zewnętrznej. Podejście DZ jest zalecane przez instytucje standaryzacyjne (łącznie z Komitetem Automatyki Przemysłowej i Systemów Sterowania (ISA-99) i międzynarodową Komisję Elektrotechniczną (IEC)), gdyż hakerzy mają znacząco utrudniony dostęp do systemów. Jaka jest zatem reakcja tych „niegrzecznych chłopców"? Obecnie hakerzy dążą do infiltracji wszelkich sieci, niemal zawsze usiłując przejąć kontrolę nad najbardziej ważnymi obiektami i punktami o uprzywilejowanym dostępie. W przypadku infrastruktury krytycznej błędy wywołane w systemach SCADA i ICS (utrata kontroli, niewłaściwe zabezpieczenie, błędne uzyskanie priorytetu i inne problemy niewłaściwego zarządzania) tworzą warunki zagrożenia bezpieczeństwa. Mając to na uwadze, przedsiębiorstwa energetyczne (lub ogólniej – przedsiębiorstwa o cechach użyteczności publicznej) muszą mieć pewność, że właściwie zabezpieczają krytyczne części swego majątku i ograniczają ryzyko ataku przez wykorzystanie warstwowej struktury dostępu do danych. Oznacza to konieczność zabezpieczenia tradycyjnych systemów IT, SCADA, ICS i ich sterowników procesowych z systemem scentralizowanego zarządzania, umożliwiającego sterowanie, kontrolowanie, monitorowanie i raportowanie o wszystkich zdalnych i uprzywilejowanych punktach dostępu do systemu.

W konsekwencji operatorzy elektrowni domagają się zinstytucjonalizowanej formy współpracy personelu w celu uniknięcia incydentów, wynikających z „czynnika ludzkiego". Należy traktować cyberbezpieczeństwo jako troskę o zdrowe warunki pracy i o bezpieczeństwo wieloaspektowe. Konieczne jest szkolenie personelu, uczulenie na możliwości ataku przez e-maile *(„phishing")* oraz kształcenie nawyku nieotwierania poczty elektronicznej nieznanego pochodzenia. Konieczne jest również wzmocnienie czujności, zwłaszcza na poziomie zarządczym, ponieważ menedżerowie nie są na ogół biegli w działaniach antyhakerskich. Można odnieść wrażenie, że podejście zainteresowanych firm polega bardziej na zapewnieniu powrotu do warunków pracy normalnej po ataku, niż na ochronie przed atakiem. Oczywiście nie należy odstępować od działań w imię poważnych środków bezpieczeństwa, wykraczając poza ramy obrony przez software poprzez zbudowanie rzeczywistej ochrony warstwami bezpieczeństwa, sieci back-up'owych, współpracujących z istniejącymi systemami, ale nie zintegrowanych z systemem SCADA, by nie oferować hakerom protokołu dostępu. Gdy oprogramowanie wykryje, że któraś z linii komunikacji (TCP/IP, GSM lub satelitarna) jest innym protokołem komunikacyjnym, to uśpiona do tej chwili, uzyskuje priorytet i może być wykorzystana jako podstawowa linia komunikacyjna. W zakresie działań przywracających stan normalny, firmy budują zwierciadlany system istniejącej infrastruktury użytkownika, umożliwiającej zdefiniowanie, które usługi funkcjonują on line w różnych scenariuszach awaryjnych. Dzięki komunikacji dwustronnej to podejście może nadawać priorytet różnym elementom systemu dostaw energii i wykorzystywać optymalizację. Gdy przedsiębiorstwo pracuje z firmami specjalizującymi się w bezpieczeństwie software'owym (np. Symantec), to istnieją wątpliwości, czy pełne bezpieczeństwo mogą zapewnić wyłącznie ściany ogniowe. Przy dublowaniu sieci zarażone mogą być wszystkie systemy, ale ich praca nie ulega kasacji, biznes jest kontynuowany i kończy się to katastrofą działań, mających w założeniu przywracać normalność.

Bezpieczeństwo w łańcuchu dostaw

Przedsiębiorstwa nie mogą troszczyć się tylko o zabezpieczenie swych działań w obrębie własnych organizacji.

Zgodnie z danymi z 2013 r. cyberryzyko wchodzi obecnie na listę najważniejszych 10 ryzyk dla przedsiębiorstw brytyjskich i w rankingu zajmuje pozycję siódmą. Pierwszym, najważniejszym z ryzyk jest przerwanie produkcji na skutek ryzyka przerwy w dostawach, w którym może być zawarty efekt cyberbezpieczeństwa. Wskazać tu można na niedawny atak na amerykańską sieć Target, dokonany poprzez łańcuch dostaw nośników ciepła, wentylacji i chłodu (HVAC). Gdy przedsiębiorstwa infrastrukturalne rozrastają się i stają coraz bardziej złożone, to są zarazem trudniejsze do zaatakowania ponieważ będą zarazem bardziej skore do inwestowania w bezpieczeństwo. Stąd hakerzy usiłują zaatakować słabiej bronione obiekty łańcucha dostaw.

Upewnić się o gotowości

Nie istnieje droga do uzyskania pełnej odporności na hakerstwo, bez względu na to, jak duże środki mogą być w ten proces zaangażowane. Przedsiębiorstwo pracujące z systemem SCADA może wydawać coraz większe środki w celu zamknięcia pętli niebezpieczeństwa ataku. Przed dekadą wydatki wynosiły 5 mln USD, 9 lat temu - 15 mln USD, przed 8 laty - 20 mln USD, a niebezpieczeństwo, że nawet jeden element zainfekowany ujawni się w systemie, występuje nadal. Tak więc producenci energii elektrycznej żądają ubezpieczenia, które zapewni pokrycie strat bez względu na ich powód, zatem ubezpieczenie również staje się coraz droższe. Lista cyberryzyk jest narastającym problemem dla przedsiębiorstw energetycznych, obejmując przerwanie produkcji, starzenie się i awaryjność sieci, utratę przychodów, uszkodzenie i zestarzenie się elektroniki, utratę wiarygodności (najbardziej bolesna) oraz kradzież danych. Konieczne jest także pokrycie strat z tytułu inwestowania w cyberbezpieczeństwo oraz zatrudnienia specjalistów do ochrony i identyfikacji źródła cyberataków. Istotną rolę odgrywają również prawnicy. Jednakże przed negocjacjami odszkodowawczymi przedsiębiorstwo musi upewnić się, czy podjęło wystarczające kroki dla własnej ochrony. Konieczne jest sporządzenie zwięzłego formularza ubezpieczenia, a następnie broker ubezpieczeniowy w oparciu o dane z rynku wyszykuje ubezpieczycieli, skłonnych do podjęcia wyspecyfikowanych rodzajów ryzyka. Teraz klient i firmy ubezpieczeniowe, korzystają z usług brokera dla wytypowania niezależnego specjalisty IT. Specjalista ten sporządza raport, upewniający ubezpieczyciela o należytym przygotowaniu przedsiębiorstwa do podjęcia cyberryzyka. Specjalista IT kontroluje szereg cech: ściany ogniowe, ochronę przeciwwirusową, zarządzanie USB, filtrację poczty elektronicznej i jej kontrolę, graniczne ściany ogniowe korporacji chroniące system SCADA, sterowanie dostępu do sieci oraz zarządzanie Windows i dostępem do systemów. Niskie notowania w przeprowadzonej ocenie wynikają m.in. z niedostatecznie adresowanej oceny ryzyka cyberataku. Godne uwagi jest spostrzeżenie, że ubezpieczenie nie jest obroną przed opisywanym ryzykiem. Przedsiębiorstwo musi mieć świadomość, że niektórzy ubezpieczyciele unikają włączenia cyberbezpieczeństwa do polityki ochrony własności. Przedsiębiorstwa muszą zrewidować swój profil ryzyka i ocenić, czy polityka przedsiębiorstwa ma zabezpieczenie odszkodowawcze.

Przygotowanie do niebezpiecznej przyszłości

Narasta liczba realizacji inwestycji w zmieniającym się otoczeniu ryzyka. Pojawiają się również dążenia do utworzenia scentralizowanej instytucji, śladem istniejącego Instytutu Operacji Energetyki Jądrowej, którego działania zmierzają do zwiększenia bezpieczeństwa w tym sektorze energetyki. Konieczna jest jednolita odpowiedź przemysłu w zakresie zarządzania ryzykiem, bezpieczeństwa, działań w warunkach zagrożenia awaryjnego, badania stanów nienormalnych i straty sterowania. Przedsiębiorstwa, działające jako struktury krytyczne, powinny otrzymywać jednolite wskazania; nikt nie tęskni za powtórzeniem sytuacji, która wynikła po cyberataku na amerykański Target, gdy regulatorzy i interesariusze stali się coraz bardziej agresywni i bezwzględni w działaniu. Jednakże rządy muszą zrozumieć, że ubezpieczenie nie może być jedynym rozwiązaniem problemu cyberryzyka. Politycy zdają się sądzić, że istnieje nieograniczony potencjał ubezpieczeń - nie jest to jednak prawdą. Ubezpieczyciele mają środki ograniczone i mogą nawet nie wchodzić w niebezpieczną - w ich mniemaniu - grę. Niezbędne jest porozumienie stron w celu lepszego zarządzania cyberryzykiem oraz modelowania ryzyka i polepszenia bezpieczeństwa. Rządy i instytucje muszą współpracować dla ochrony najbardziej wrażliwego majątku i obserwujemy z ulgą, iż tak zaczyna się to już dziać. Przykładem jest sytuacja w USA, gdzie rząd opublikował dokument o ramowych zasadach cyberbezpieczeństwa (Cybersecurity Framewerk) dla elektrowni, przedsiębiorstw gospodarki wodnej i innych przedsiębiorstw infrastruktury. Dokument ten wprowadza nową jakość do polityki ubezpieczeniowej z uwzględnieniem cyberbezpieczeństwa dla ważnych przedsiębiorstw, w tym energetycznych. Cechą tego podejścia jest „obrona pierwszej linii", co również jest właściwością nowego brytyjskiego programu treningu w zakresie cyberbezpieczeństwa, opracowanego przez Rządowe Kolegium Planowania Kryzysowego. Program Cybx jest symulatorem do szkolenia personelu technicznego w warunkach pozorowanego cyberataku. Program oddaje realia ataku z użyciem najnowszego oprogramowania i skrajnych wartości parametrów tego ataku. Uczestnictwo w szkoleniu certyfikowane jest świadectwem uzyskania kwalifikacji.

Poważny biznes

Konsekwencje cyberataków mogą być szczególnie poważne dla przedsiębiorstw związanych z energią. Wiele problemów wynika przy modernizacji systemów SCADA w przedsiębiorstwach, zwłaszcza gdy chodzi o systemy bardzo stare, stwarzające kłopoty ze stabilnością. Ilustrować to może przykład wzięty z praktyki zarządzania platformą wiertniczą w przemyśle naftowym: modernizacja oprogramowania polega na pełnej wymianie softwer'u. W następstwie tych działań, kilka dni później następuje eksplozja z katastrofalnymi skutkami dla środowiska. W terminologii ubezpieczeń w czasie od rozpoczęcia wymiany oprogramowania aż po niezamierzone jej skutki mamy okres, w którym obiekt nie kwalifikuje się do ubezpieczenia, nie istnieje bowiem na tym rynku dostateczny potencjał dla podjęcia działań typu „insurance". Konieczne jest zrozumienie wagi tego zjawiska: tylko w 2013 r. realny skutek cyberataków na przemysłowe systemy sterowania w skali światowej w 5% tych działań hakerskich prowadził do skutków śmiertelnych w najbliższym otoczeniu. Podczas gdy atak na komputer w obszarze IT skutkuje w najgorszym przypadku utratą możliwości korzystania z poczty elektronicznej, to w

przypadku przemysłu dostaw energii - skutkiem może być utrata życia przez personel obsługi i eksploatacji w kluczowym obecnie sektorze gospodarki. Jeżeli cyberatak prowadzi do wprowadzenia do software'u fałszywych danych o historii procesu i przesłanie ich do systemu alarmowania, to w rezultacie nastąpi demontaż działań w procesie wykrywania i kasowania błędów. Możliwe jest wówczas nieprawidłowe zadziałanie, a w przypadku scenariusza najgorszego - spowodowanie dramatycznego wypadku. „Potrzebne jest przebudzenie w obliczu zagrożeń rodem z literatury science fiction, które stały się rzeczywistością. Wszyscy muszą uczestniczyć w ograniczaniu konsekwencji tego rodzaju problemów - dziś obserwujemy dopiero pierwsze symptomy niebezpieczeństwa, ale świat się zmienia i musimy nadążać za tymi zmianami"- taka jest konkluzja rozważań T. Bayar'a.

Post Scriptum

16 stycznia 2015 r. światowe agencje informacyjne przekazały za brytyjską ITV komunikat „Brytyjska Agencja Wywiadu Elektronicznego GCHQ i amerykańska Agencja Bezpieczeństwa Narodowego NSA powołają do życia specjalną komórkę wywiadu dla przeciwdziałania cyberatakom na infrastrukturę informacyjną, portale rządowe i banki centralne. Będą one prowadzić ćwiczenia symulacyjne dla zbadania scenariuszy możliwych ataków w celu zapobiegania wykorzystania Internetu do działań terrorystycznych". Premier UK D. Cameron stwierdził ponadto, że „punkt ciężkości w komunikacji elektronicznej musi (…) przesunąć się od obrony prywatności w stronę prewencji antyterrorystycznej".

T. Bayar: Cybersecurity in the Power sector. Power Eng. Intern. Vol. 22, Iss. 9, Oct. 2014