TECHNIKA TRANSPORTU SZYNOWEGO

Teresa MENDYK-KRAJEWSKA, Zygmunt MAZUR

WYBRANE ASPEKTY BEZPIECZEŃSTWA ZAKŁADOWYCH SYSTEMÓW INFORMATYCZNYCH

Streszczenie

Jedną z przyczyn naruszeń bezpieczeństwa systemów informatycznych są błędy oprogramowania, które można wykorzystać, by uzyskać nielegalny dostęp do danych lub całkowicie przejąć kontrolę nad systemem. Problem ten dotyczy także nie pozbawionych wad sieci przemysłowych (przede wszystkim z powodu coraz częstszego ich łączenia z zakładowymi sieciami informatycznymi) i jest poważny, z powodu skali zjawiska i braku radykalnych rozwiązań. W ostatnim okresie obserwuje się wzrost zagrożeń dla bezpieczeństwa systemów zakładowych i sieci przemysłowych, których skutki mogą być bardzo groźne.

WSTĘP

Jedną z przyczyn naruszeń bezpieczeństwa systemów informatycznych stanowią wady oprogramowania wynikające z błędów programistycznych, niedostatecznego testowania finalnych produktów i nieprawidłowej konfiguracji systemów. Problem istnienia luk1 umożliwiających atakowanie systemu dotyczy wszystkich rodzajów oprogramowania, lecz na ataki z ich wykorzystaniem najbardziej narażone są systemy powszechnie stosowane (z powodu łatwości ich penetracji oraz opłacalności tworzenia narzędzi do przeprowadzenia ataku) oraz te, które są celem strategicznym (na przykład systemy sterowania w sieciach przemysłowych).

Sposób przeciwdziałania niekorzystnemu zjawisku polegający na udostępnianiu nakładek systemowych lub tworzeniu lepiej zabezpieczonych wersji oprogramowania jest zabiegiem uciążliwym, kosztownym i stanowi jedynie krótkotrwałe rozwiązanie problemu.

Ważny jest też czas między wykryciem luki a opracowaniem dla niej poprawki.

[1] Pod pojęciem luki należy rozumieć taki stan systemu komputerowego, który umożliwia dostęp do danych, wykonywanie poleceń w imieniu uprawnionego użytkownika oraz prowadzenie bezprawnej działalności.

1. PROBLEM WAD OPROGRAMOWANIA SYSTEMÓW KOMPUTEROWYCH

1.1. Zagrożenia

Wyróżnia się wiele typów luk: są to pliki przykładów, ujawnienie kodu źródłowego, rozszerzenia serwera czy błędy w zatwierdzaniu danych wejściowych. Najbardziej niebezpieczne są te, które umożliwiają przejęcie kontroli nad systemem (luki krytyczne).

Do atakowania systemu z wykorzystaniem wad oprogramowania tworzone są specjalne programy (tzw. exploity), ale mogą być też użyte różne szkodliwe kody. Przykładowo, znane luki wykorzystują robaki, takie jak Blaster (umożliwia przepełnienie bufora stosu w interfejsie RPC[2]), Sircam (wykorzystuje lukę w usłudze stacji roboczej systemu Windows) lub Conficker (wykorzystujący głównie luki w zabezpieczeniach systemu Windows Server) oraz konie trojańskie (np. URLZone atakujący konta w e-bankach dzięki lukom w zabezpieczeniach przeglądarek).

Niestety, czas od chwili ujawienia luki do jej usunięcia może być długi, dlatego krytykowane jest przedwczesne upublicznianie informacji o tego typu zagrożeniach.

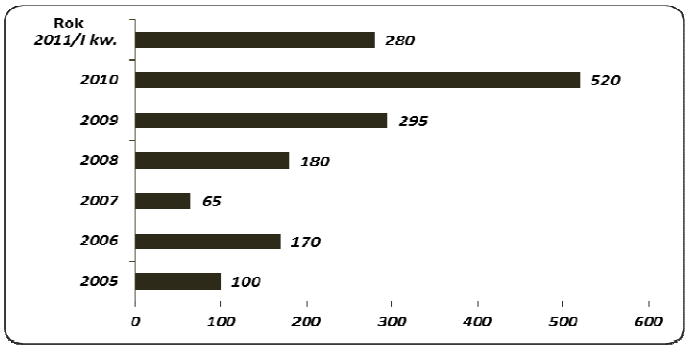
Z badań wynika, że największa liczba udanych ataków jest możliwa ze względu na luki w kilku popularnych usługach sieciowych zaimplementowanych w systemach operacyjnych oraz błędy w podstawowym oprogramowaniu użytkowym.

Oprogramowanie używane w sieciach przemysłowych nie jest pozbawione błędów podobnych do tych wykrywanych w powszechnie stosowanym. O lukach w systemach SCADA[3] pisano od dawna, jednak długo nie dostrzegano niebezpieczeństwa. Systemy te projektowano bowiem z myślą o funkcjonowaniu w wyizolowanych sieciach sterujących ruchem kolejowym, procesami przemysłowymi w fabrykach (linie montażowe), elektrowniach (sieci energetyczne), w zakładach chemicznych itd. Przemysłowe systemy sterowania ICS (*Industrial Control System*) charakteryzowały się specjalizowanym sprzętem i oprogramowaniem, wydzielonymi kanałami komunikacyjnymi oraz brakiem połączeń pomiędzy różnymi ICS, i funkcjonowały niezależnie od sieci teleinformatycznych. Utrudniona dostępność tych systemów uniemożliwiała ich penetrację.

Jedną z przyczyn wzrostu zagrożenia dla sieci zakładowych, w tym sieci przemysłowych, jest stosowanie podatnych na ataki rozwiązań bezprzewodowych oraz coraz bardziej powszechny dostęp do zasobów firmowych z urządzeń mobilnych (np. smartfonów), które również stały się przedmiotem zainteresowania hakerów. O niepokojącym tempie wzrostu zagrożeń dla urządzeń mobilnych świadczy notowany w ostatnich latach przyrost wzorców w bazach wirusów ich oprogramowania ochronnego (rys. 1) [18].

Do wykorzystywania luk w systemach SCADA są opracowywane exploity, zaś skutecznie przeprowadzony atak może prowadzić do przejęcia kontroli nad sprzętem i sterowanymi procesami. Spośród robaków największe zagrożenia dla sieci zakładowych niosą Stuxnet, Duqu, Flame i Gauss. Skutkiem może być wywołanie awarii, unieruchomienie lub zniszczenie obiektów gospodarczych i użyteczności publicznej (systemów energetycznych, sygnalizacji świetlnej, instalacji wodociągowych, systemów obsługujących transport, zapory wodne czy szpitale).

[2] *Remote Procedure Call* – protokół zdalnego wywoływania procedur.
[3] *Supervisory Control And Data Acquisition* – rozproszony system elementów wykonawczych i monitorujących, połączonych z centrami dyspozycyjnymi przez rozległe sieci telekomunikacyjne, nadzorujący przebieg procesu technologicznego lub produkcyjnego.



Rys. 1. Liczba nowych sygnatur w bazie wirusów oprogramowania ochronnego firmy Kaspersky

Ważne jest, by aktualizacje były pobierane z oficjalnych stron producentów oprogramowania. Niejednokrotnie informowano o udostępnianiu w Internecie fałszywych nakładek systemowych bądź zaktualizowanych aplikacji – na przykład podczas wyszukiwania nowej wersji dla programu Flash Player firmy Adobe, na pierwszym miejscu ukazywał się link do podrobionej strony z plikiem do pobrania, który w rzeczywistości był wirusem z rodziny Win32.Agent.

W celu zapewnienia wysokiej jakości wytwarzanego oprogramowania opracowano wiele norm, standardów i zaleceń. Wśród licznych tego typu dokumentów warto wymienić: ISO/IEC 9126, ISO/IEC 14598, ISO/IEC 15939, ISO/IEC 25000 (SQuaRE) oraz ISO/IEC 15504 [11].

1.2. Skala zjawiska

Najbardziej popularnym, zatem często atakowanym oprogramowaniem, jest system operacyjny Windows firmy Microsoft, a wykrywane luki dotyczą: serwera i usług WWW, usługi stacji roboczej, usługi zdalnego dostępu, serwera MS SQL, przeglądarki WWW, mechanizmu uwierzytelniania, aplikacji wymiany plików, klienta poczty elektronicznej czy komunikatorów internetowych (*Instant Messenger*). Z kolei w systemach Unix najczęściej wykorzystywane luki dotyczą między innymi: serwera nazw BIND (*Berkeley Internet Name Domain*), serwera WWW, procesu uwierzytelniania, serwera pocztowego, protokołu SNMP (*Simple Network Management Protocol*) oraz samego jądra [1].

Podatne na ataki są również popularne aplikacje użytkowe, takie jak: programy do obsługi poczty elektronicznej, edytory tekstowe, arkusze kalkulacyjne, programy prezentacyjne, oprogramowanie firmy Adobe (Acrobat, Reader, Flash, Photoshop) oraz odtwarzacze plików multimedialnych (Apple Quick Time, Real Player firmy Real Networks, Windows Media Player czy Realtek Media Player).

Producenci oprogramowania systematycznie publikują biuletyny bezpieczeństwa informując o zagrożeniach i opracowanych poprawkach. Zależnie od ich znaczenia, lukom nadaje się odpowiedni status: krytyczna, ważna, umiarkowana. Skalę zjawiska obrazuje częstość wykrywania luk i liczba udostępnianych nakładek systemowych. Przykładowo, w lipcu 2012 roku firma Oracle w Critical Patch Update zamieściła aż 87 poprawek dla wielu swoich produktów, między innymi dla Oracle Database Server – 4, Oracle Secure Backup – 2, Oracle E-Business Suite – 4, Oracle PeopleSoft Products – 9 i dla Oracle MySQL – 6 poprawek [13]. W tym samym miesiącu Firma Microsoft w publikowanym biuletynie bezpieczeństwa informowała o usunięciu dziewięciu błędów – trzy aktualizacje posiadają status „krytyczny" (w czerwcu było takich przypadków 7), a sześć zostało sklasyfikowanych jako „ważne". Wśród poprawek o krytycznym znaczeniu wymienia się:

- MS12-043 – *Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution* (2722479) – dotyczy podatności w Microsoft XML Core Services,
- MS12-044 – *Cumulative Security Update for Internet Explorer* (2719177) – dotyczy dwóch luk w programie Internet Explorer,
- MS12-045 – *Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution* (2698365) – aktualizacja zabezpieczeń Microsoft Data Access Components (luka krytyczna dla Windows XP, Vista oraz Windows 7).

Wykryte luki umożliwiają atakującemu zdalne wykonanie kodu po wejściu użytkownika na spreparowaną stronę WWW.

W przypadku sieci przemysłowych, już w 2008 roku ostrzegano przed poważną luką w wykorzystywanym w około 30% zakładów na świecie oprogramowaniu *InTouch SuiteLink* firmy Invensys dla systemu Windows, kontrolującym systemy przemysłowe. Błąd w komponencie *SuiteLink Service* umożliwiającym (dla przesłania danych) łączenie własnych protokołów ze standardem TCP/IP umożliwia atakującemu (przy pomocy specjalnie przygotowanego pakietu) zdalne wyłączenie systemu SCADA. W tym samym roku ujawniono też lukę umożliwiającą zdalny nieuprawniony dostęp, a w konsekwencji przejęcie kontroli nad systemem, w oprogramowaniu CitectSCADA, co naraża na niebezpieczeństwo systemy z sektorów: kosmicznego, produkcyjnego, naftowego, gazowego i użytku publicznego. Aplikacja CitectSCADA obsługuje otwarte łącza baz danych ODBC[4] (*Open DataBase Connectivity*) umożliwiające dostęp z wykorzystaniem poleceń SQL do systemów bazodanowych. Luka polega na braku skutecznego mechanizmu kontroli długości strumienia pobieranych danych, czego skutkiem jest przepełnienie bufora stosu (*stack-based buffer overflow*) [2].

We wrześniu 2009 roku doniesiono o wykryciu problemów związanych z szyfrowaniem danych podczas procesu uwierzytelniania użytkowników w systemie OSIsoft PI Server (podatne na atak są wszystkie wersje). Wykorzystując lukę można uzyskać dostęp do poufnych informacji operacyjnych oraz zmodyfikować lub usunąć dane z serwera. Producent nie planował publikowania poprawki.

W marcu 2011 roku na liście dyskusyjne seclists.org informowano o 24 lukach w systemach SCADA dostarczonych przez różnych producentów (m.in. Siemens, Iconics, 7-Technologies oraz DATAC). Wiosną tegoż roku na prośbę przedstawicieli Departamentu Bezpieczeństwa Wewnętrznego USA oraz firmy Siemens odwołano planowaną prezentację poświęconą bezpieczeństwu systemów SCADA. Podczas konferencji eksperci z firmy NSS Labs mieli przedstawić techniki umożliwiające przeprowadzenie skutecznego ataku na najlepiej chronione systemy przemysłowe na świecie oraz pokazać sposoby tworzenia dla nich szkodliwego oprogramowania bez dostępu do atakowanego sprzętu. Upublicznienie informacji wstrzymano na czas poprawienia błędów, by nie potęgować zagrożenia [3].

W połowie 2011 roku informowano o luce (błąd przepełnienia stosu w kontrolce ActiveX używanej przez SCADA) dotyczącej niektórych wersji produktów Genesis 32 i BizViz korporacji Iconics, umożliwiającej zdalne wykonanie kodu (aplikacje używane w systemach sterujących w fabrykach, elektrowniach, rafineriach, oczyszczalniach ścieków itd.) [4]. Z kolei jesienią 2011 roku doniesiono o kolejnych kilkunastu błędach wykrytych w oprogramowaniu firm Beckhoff, Measuresoft, Rockwell, Carel, Progea, AzeoTech oraz Cogent, używanym w przemyśle zbrojeniowym, lotniczym i kosmicznym [5]. W grudniu informowano o zagrożeniach związanych z wykrytą wcześniej luką w oprogramowaniu SIMATIC, które zarządza systemami automatyki przemysłowej. W tym przypadku problem dotyczy domyślnego hasła administratora dla usług Web, VNC i Telnet oraz tokenów sesji, które nie mają dostatecznie losowego charakteru.

[4] Interfejs pozwalający programom łączyć się z systemami zarządzającymi bazami danych; w skład ODBC wchodzą wywołania wbudowane w aplikacje oraz sterowniki.

Według specjalistów, bardzo podatne na ataki jest oprogramowanie KingView SCADA firmy WellinTech Inc. powszechnie instalowane w sieciach przemysłowych w Chinach [6]. Wykryty przez amerykańskiego specjalistę błąd w tym systemie został poprawiony dopiero po kilku miesiącach od jego opublikowania.

1.3. Przyczyny wzrostu zagrożenia dla sieci przemysłowych

Występowanie luk w systemach SCADA nabrało istotnego znaczenia z powodu zmiany charakteru sieci przemysłowych. Systemy przemysłowe[5] cechują się pewnym ściśle określonym czasem reakcji na zdarzenia, wysoką niezawodnością oraz realizacją określonych procedur w przypadku awarii. Zagrożeniem dla nich są zarówno zakłócenia działania czujników czy elementów wykonawczych, jak i modyfikacja danych lub nieuprawniony dostęp do systemu. Obserwowany znaczący wzrost zagrożeń dla ich bezpieczeństwa spowodowany jest przede wszystkim wykorzystywaniem aplikacji komercyjnych (zamiast rozwiązań indywidualnych) oraz używaniem (do sterowania i zarządzania) powszechnie stosowanych kanałów komunikacyjnych (ułatwiając nieuprawniony dostęp do sieci), a także podłączaniem komputerów zakładowych do Internetu. Ponadto, systemy ICS są coraz częściej na obszarze danego przedsiębiorstwa, z różnych przyczyn (np. z powodu potrzeby dostępności danych dla systemów wspomagających zarządzanie), łączone z systemami teleinformatycznymi stosowanymi powszechnie. Przy tym, długo eksploatowane, nie są w stanie obsłużyć dodatkowych zadań związanych z bezpieczeństwem (ze względu na ograniczenie pamięci i mocy obliczeniowej).

Na ogół systemy SCADA skonfigurowane w okresie rozruchu nie są później aktualizowane, ponieważ w praktyce jest to trudne do wykonania (wiąże się z przerwaniem pracy systemu lub koniecznością duplikacji obiektów przemysłowych).

Systemy SCADA narażone są też na ryzyko z powodu dołączanego dodatkowego oprogramowania (np. raportującego, analizującego, archiwizującego, kontrolek ActiveX, komunikatorów).

Wiele instalacji SCADA nie jest dostępnych z sieci zewnętrznych, lecz mogą ulec zainfekowaniu poprzez zewnętrzne nośniki pamięci (na przykład pendrive'y).

2. ATAKOWANIE SYSTEMÓW PRZEMYSŁOWYCH

Ze względu na duże zagrożenie dla bezpieczeństwa sieci energetycznych istnieje konieczność zabezpieczania linii przesyłowych, elektrowni oraz sieciowych systemów komputerowych. Użytkowane oprogramowanie często nie jest aktualizowane, brak jest dostatecznej ochrony informacji o dostawcach i odbiorcach (zabezpieczenia kryptograficzne są słabe lub w ogóle nie są stosowane), niedostateczna jest też ochrona dostępności sieci. Jednocześnie tworzona jest koncepcja inteligentnych sieci energetycznych integrujących małe alternatywne źródła energii (panele słoneczne, turbiny wiatrowe). Ta zaawansowana infrastruktura informatyczna dla osiągnięcia większej wydajności i skutecznej kontroli łączona jest z Internetem. Tymczasem, na przykład używanie publicznych adresów IP liczników energii elektrycznej czyni je podatnymi na ataki odmowy usługi DoS (*Denial of Service*), czego skutkiem może być na przykład odcięcie odbiorcy dostawy prądu.

W 2010 roku dokonano ataku na irańskie sieci przemysłowe (w tym komputery elektrowni atomowej w Buszehr) przy pomocy programu Stuxnet[6] (Trojan-Dropper.Win32.Stuxnet, Rootkit.Win32.Stuxnet.a), zarażając nim 60% komputerów. Był to

[5] Główne elementy systemów przemysłowych to specjalizowany sprzęt komputerowy, sterowniki, urządzenia wejścia/wyjścia oraz media komunikacyjne.

[6] Posiadał sygnaturę cyfrową; znane są różne warianty sterownika Stuxnet'a, m. in. Mrxcls.sys i Mrxnet.sys (powstały odpowiednio w latach 2009 i 2010).

pierwszy szkodliwy kod, który na taką skalę zaatakował systemy sterowania – umożliwiając podsłuch (kontrolę produkcji) i modyfikację instalacji przemysłowych (parametrów pracy urządzeń). Drogą infekowania systemów jest rzekomo port USB, co nie uzasadnia szybkiego rozprzestrzeniania się kodu, stąd podejrzenie, że może nią być nieznana dotąd metoda. Zaatakowanych zostało też tysiące systemów zakładowych w innych krajach azjatyckich. Stuxnet atakuje systemy z oprogramowaniem WinCC, wyszukując w sieci określony programowalny sterownik logiczny (PLC) firmy Siemens (efektem jest modyfikacja jego działania z wykorzystaniem luki). Urządzenia firmy Siemens są stosowane w zakładach przemysłowych na całym świecie, między innymi w elektrowniach, rafineriach ropy naftowej, oczyszczalniach ścieków i zakładach nuklearnych. Robak ma ułatwione zadanie, gdyż baza danych stanowiąca podstawę działania systemów przemysłowych ma we wszystkich instalacjach takie same dane logowania. Ogromne koszty poniesione na opracowanie tego kodu (jego złożoność, wykorzystywane techniki i aż cztery luki typu zero-day[7] oraz warunki testowania) wskazują na polityczny cel ataku.

W 2011 roku doniesiono o wykryciu kolejnego zagrożenia dla instalacji przemysłowych – robaka Duqu (wykorzystującego lukę w jądrze systemu Windows[8]), którego zadaniem jest zbieranie danych w celu przeprowadzenia na nie ataku. Był on zaopatrzony w certyfikat (już unieważniony) i kod powodujący jego autodestrukcję po określonej liczbie dni od infekcji systemu. Według analityków z Kaspersky Lab, Stuxnet i Duqu stanowią dwa równoległe projekty tych samych autorów [7].

W 2012 roku pojawił się zaawansowany robak Worm.Win32.Flame, który potrafi pobierać dane różnymi metodami, przesyłać je w postaci zakodowanej i rozprzestrzeniać się na wiele sposobów [9].

Na początku 2011 roku były pracownik firmy NextEra Energy Reseurces dowodził na poświęconej zabezpieczeniom liście mailingowej Full Disclosure, że uzyskał dostęp do panelu kontrolnego systemu turbin na farmie wiatrakowej w stanie Nowy Meksyk zarządzanego przez tę firmę [8]. Według ekspertów, przedstawione przez niego materiały nie stanowią dowodu, jednak potwierdzają możliwość wyłączenia, a nawet uszkodzenia turbin wiatrakowych. Atakowanie systemów przez pracowników nie jest rzadkością – jak wykazały badania, w USA co dziesiąty atak informatyczny na firmę został dokonany przez jej byłego pracownika.

W listopadzie 2011 roku jeden z hakerów ogłosił, że jest w stanie przejąć kontrolę nad siecią publicznych wodociągów w USA. Według władz zaistniała awaria pompy systemu dostarczania wody w stanie Illinois nie była wynikiem ataku, jednak zdaniem ekspertów taka możliwość istnieje. W tym samym roku doniesiono o zmasowanym ataku na norweskie koncerny paliwowe i energetyczne. Hakerzy wysyłali do pracowników wybranych zakładów listy elektroniczne zawierające szkodliwy kod umożliwiający zdalne przejęcie kontroli nad systemem, dzięki czemu mogli uzyskać dostęp do tajnych dokumentów tych firm [16].

Celem ataku stał się też Mitsubishi Heavy Industries (należący do japońskiej grupy Mitsubishi) będący producentem, między innymi, urządzeń dla wojska oraz sektorów energetycznego i stoczniowego. Kilkadziesiąt komputerów firmy zostało zaatakowanych wirusem, jednak zdaniem jej przedstawicieli, żadne poufne dane dotyczące produktów oraz stosowanych technologii nie zostały ujawnione [17].

Podane przykłady nie wyczerpują listy możliwości atakowania systemów przemysłowych, ale wskazują na realne zagrożenia dla infrastruktury krytycznej krajów.

Systemy SCADA wymagają instalacji specjalnego oprogramowania ochronnego, nie zakłócającego ich pracy i minimalnie obciążającego zasoby systemowe. Przykładem takiego narzędzia może być Endpoint Protection norweskiej firmy Norman [12].

[7] Luka zero-day – nowo odkryta wada, dla której nie została jeszcze opracowana poprawka.
[8] Robak dociera do systemu wykorzystując specjalnie spreparowany plik programu Word.

3. WYBRANE NORMY I STANDARDY BEZPIECZEŃSTWA

Problemy z zapewnieniem bezpieczeństwa systemom komputerowym mogą mieć wszyscy, którzy nimi administrują. W celu jak najlepszego ich zabezpieczenia opracowywane są normy i standardy dla sprzętu, oprogramowania, procesów projektowania i wytwarzania oprogramowania, administrowania systemem, polityki bezpieczeństwa itd.

Ze względu na bardzo szeroki zakres, jaki musi być objęty kontrolą, wykaz norm i standardów również jest bardzo obszerny. Na uwagę zasługuje siedem części normy PN-EN 61508 [10] dotyczącej procesu wytwarzania (a nie jakości produktu):

- PN-EN 61508-1:2010 *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 1: Wymagania ogólne*, która obejmuje zagadnienia związane z opracowaniem systemów elektrycznych, elektronicznych oraz programowalnych elektronicznych wiążących się z bezpieczeństwem, dla których nie ma norm międzynarodowych dotyczących sektorów zastosowań,
- PN-EN 61508-2:2010 *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 2: Wymagania dotyczące elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem*; wyszczególniono tu wymagania dotyczące czynności, które mają być wykonane podczas projektowania i wytwarzania systemu elektrycznego, elektronicznego lub programowalnego elektronicznego wiążącego się z bezpieczeństwem, oraz podano informacje konieczne do zainstalowania systemu oraz przeprowadzenia odbioru komisyjnego i walidacji jego bezpieczeństwa,
- PN-EN 61508-3:2010 *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 3: Wymagania dotyczące oprogramowania*; w dokumencie opisano wymagania odnośnie dowolnego oprogramowania stanowiącego część systemu mającego związek z bezpieczeństwem,
- PN-EN 61508-4:2010 *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 4: Definicje i skrótowce*; podano tu definicje, wykaz skrótowców oraz terminów w języku polskim i angielskim stosowanych w przypadku elektronicznych systemów związanych z bezpieczeństwem,
- PN-EN 61508-5:2010 *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa* – w tej części zawarto zagadnienia dotyczące ryzyka i jego związku z poziomem nienaruszalności bezpieczeństwa,
- PN-EN 61508-6:2010 *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3*; dokument zawiera m.in. wskazówki dotyczące stosowania części 2 i 3 normy IEC 61508, opisy przykładowych technik obliczania prawdopodobieństwa uszkodzenia sprzętu i przykłady zastosowania tablic nienaruszalności bezpieczeństwa oprogramowania,
- PN-EN 61508-7:2010 *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 7: Przegląd technik i miar*; w normie przedstawiono przegląd technik i miar bezpieczeństwa odnoszących się do części 2 i 3 normy IEC 61508.

Oprócz opisanej normy PN-EN 61508 można wymienić wiele innych, między innymi:

- PN-EN 61511 *Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego*:

  - *Część 1 (2007): Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania,*
  - *Część 2 (2008): Wytyczne do stosowania IEC 61511-1,*
  - *Część 3 (2009): Wytyczne do określania poziomów wymaganych nienaruszalności bezpieczeństwa,*
- PN-EN ISO 13849 *Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego*:
  - *Część 1 (2008): Ogólne zasady projektowania,*
  - *Część 2 (2008): Walidacja,*
- PN-EN 61499 *Bloki funkcjonalne*:
  - *Część 1 (2006): Architektura,*
  - *Część 2 (2006): Wymagania dotyczące narzędzi programowych,*
  - *Część 4 (2006): Reguły do profili zgodności,*
- PN-EN 61918:2008 *Przemysłowe sieci komunikacyjne – Instalowanie sieci komunikacyjnych w obiektach przemysłowych*,
- PN-EN 61784 *Przemysłowe sieci komunikacyjne – Profile,*
- EN 62061 PN-EN 62061:2008/AC:2011 *Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem*.

Ocena bezpieczeństwa systemów programowalnych jest zagadnieniem trudnym, głównie ze względu na duże rozmiary kodów źródłowych i złożoność procesu testowania. Trudno jest wykazać, że system z całą pewnością nie posiada błędów, stąd też nieraz wiele z nich ujawnia się w specyficznych warunkach eksploatacyjnych, po wielu latach użytkowania. Dostarczane normy umożliwiają stosowanie jednolitych metod oceny bezpieczeństwa systemów komputerowych. Zawierają też wskazówki umożliwiające zarządzanie polityką bezpieczeństwa oraz właściwe dokumentowanie etapów projektowania obwodów realizujących funkcję bezpieczeństwa.

Po pozytywnym wyniku badania zgodności procesu wytwarzania urządzenia (elektrycznego, elektronicznego bądź mechanicznego) z wymaganiami norm PN-EN 61508 i/lub PN-EN 61511 (bądź innych norm wydanych na bazie norm podstawowych PN-EN 61508) wydawany jest certyfikat SIL (*Safety Integrity Level*)[9] określający poziom nienaruszalności bezpieczeństwa urządzenia [14]. Jest on poświadczeniem spełnienia wymagań formalnych i technicznych (parametrów niezawodnościowych wyrobu). W zależności od obszaru zastosowania (np. sterowanie ruchem ulicznym, kolejowym czy produkcją), wymagany jest odpowiedni poziom SIL. Przykładowo, w systemach sterowania ruchem kolejowym musi być SIL4 – zgodnie z wymaganiami określonymi w normie EN 50129 *Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem*. Ocena bezpieczeństwa, wymagania dotyczące bezpieczeństwa z uwzględnieniem norm PN-EN 61508/PN-EN 61511, a także graf ryzyka zostały omówione w [15].

PODSUMOWANIE

Mimo nieustających wysiłków na rzecz wzrostu poziomu ochrony systemów teleinformatycznych, zagrożenie dla bezpiecznego ich użytkowania wcale nie maleje.

Użytkownicy nie zawsze dostatecznie dbają o aktualizację systemów, choć do kontroli poziomu ich ochrony, w tym instalacji nakładek, służy wiele narzędzi, np. Personal Software Inspector i Network Software Inspector firmy Secunia, czy popularne oprogramowanie testujące poziom zabezpieczeń, jak Nessus czy MBSA (*Microsoft Baseline Security*

[9] Wyróżnia się cztery poziomy SIL: od SIL 1 – najniższy do SIL 4 – najwyższy.

Analyzer). Między innymi z tego powodu wadliwe wersje oprogramowania są stosowane dość powszechnie.

Problem zagrożenia bezpieczeństwa w nie mniejszym stopniu dotyczy również sieci zakładowych, w tym sieci przemysłowych. Szczególny niepokój budzi możliwość nieuprawnionego ingerowania w systemy SCADA, tym bardziej, iż obserwuje się, że ataki na infrastruktury o znaczeniu krytycznym i wielkie korporacje stają się (oprócz ataków na sieci rządowe) głównym celem przestępców sieciowych.

Prowadzone badania nad ochroną infrastruktury informatycznej w przemyśle wymagają intensyfikacji i zwiększenia nakładów finansowych. Wobec narastającego zagrożenia dla sieci zakładowych, a w szczególności sieci przemysłowych, instytucje standaryzujące stają przed ważnym zadaniem opracowania nowych i aktualizowania obowiązujących dokumentów normatywnych i standaryzacyjnych, co wymaga ścisłej współpracy z zainteresowanymi sektorami, producentami sprzętu oraz oprogramowania.

SELECTED ASPECTS OF THE SECURITY OF CORPORATE IT SYSTEMS

Abstract

One of the sources of breaching the security of IT systems lies in software faults that can be used to gain unauthorized access to data or to take over the control over the system. This problem also concerns industrial networks (mostly because of more popular integration with corporate networks) and is quite serious given its extent and the lack of radical solutions. Most recently we have witnessed the increase of threats for the security of corporate and industrial networks, which may result in severe consequences.

BIBLIOGRAFIA

1. McClure S., Scambray J., Kurtz G.: *Hacking zdemaskowany. Bezpieczeństwo sieci – sekrety i rozwiązania*. Warszawa, Wydawnictwo Naukowe PWN S.A. 2006.
2. www.automatyka.pl/newsItem.aspx?pk=5222 (26.06.2008).
3. www.theregister.co.uk/2011/05/19/scada_vuln_talk_cancelled (19.05.2011).
4. http://hacking.pl/pl/news-16404-Powazna_luka_w_sofcie_SCADA.html (13.05.2011).
5. http://kopalniawiedzy.pl/SCADA-dziura-luka-Stuxnet-Luigi-Auriemma-13916.html (16.09.2011).
6. Smithson S.: *China open to cyber-attack. Vulnerability of dams, pipelines lies in software*. The Washington Times, washingtontimes.com/news/2011/mar/17/china-open-to-cyber-attack/?page=1 (17.03.2011).
7. www.viruslist.pl/analysis.html?newsid=692 (03.01.2012).
8. Steliński A.: *Atak hakerski na elektrownie wiatrowe?* www.networld.pl/news/369336/ Atak.hakerski.na.elektrownie.wiatrakowe.html (18.04.2011).
9. *The Flame: Questions and Answers*. www.securelist.com/en/blog/208193522 (28.05.2012).
10. Polski Komitet Normalizacyjny, www.pkn.pl, 2012.
11. Mazur Z., Mazur H.: *Ocena jakości systemu informatycznego*. Logistyka 2011, nr 6, s. 2461-2470.
12. www.norman.com/products/endpoint_protection/en (10.08.2012).
13. www.oracle.com/technetwork/topics/security/cpujul2012-392727.html (17.07.2012).

14. udt.gov.pl/HTML/index.php?option=com_content&task=view&id=316&Itemid=237 (10.08.2012).
15. *Bezpieczeństwo funkcjonalne w inżynierii procesowej*. *PN-EN 61508/PN-EN 61511 – ograniczanie ryzyka awarii przy użyciu przyrządowych systemów bezpieczeństwa*. https://portal.endress.com/wa001/dla/50005126204/000/00/BroszuraEHSIL_web.pdf (10.07.2012).
16. Chirgwin R.: *Phishers net Norwegian secrets. E-mail trojans sweep hard driver*. www.theregister.co.uk/2011/11/17/noway_data_theft_attack, 2011.
17. *Japan's defense industry hit by its first cyber attack*. Reuters, Tokyo 2011, www.reuters.com/article/2011/09/19/us-mitsubishiheavy-computer-idUSTRE78I0EL20110919.
18. Namiestnikow J.: *Ewolucja zagrożeń IT w I kwartale 2011 roku*. www.fixitpc.pl/topic/4351-kaspersky-lab-ewolucja-zagrozen-it-w-i-kwartale-2011 (09.06.2011).

Autorzy:
dr inż. Teresa MENDYK-KRAJEWSKA – Politechnika Wrocławska
dr hab. Zygmunt MAZUR, prof. ndzw. – Politechnika Wrocławska