Monika Adamczyk, Niezależny Ekspert, Europejska Rada ds. Innowacji (EIC)

Dlaczego cyberbezpieczeństwo przemysłowe różni się od cyberbezpieczeństwa biurowego?

Ze względu na przytłaczającą obecność systemów informatycznych i komputerów w każdym aspekcie naszego życia i coraz łatwiejszy dostęp do zaawansowanych technologii oprogramowania i sprzętu, konieczność zapewnienia bezpieczeństwa informacji i komputerów występuje w dzisiejszych czasach na porządku dziennym.

Większości ludzi cyberbezpieczeństwo kojarzy się przede wszystkim z zainstalowanym na ich osobistych komputerach i urządzeniach mobilnych oprogramowaniem antywirusowym. Nie zdają sobie oni często sprawy, że jest to dziedzina, która zajmuje się szeroką gamą środków ochrony przeciw cyberatakom dla wszystkich rodzajów systemów informatycznych. Należą do nich nie tylko nasze telefony komórkowe czy laptopy, ale także mikroprocesory w sprzęcie AGD oraz komputery sterujące i monitorujące urządzenia przemysłowe, które są odpowiedzialne za ich właściwe i bezpieczne funkcjonowanie.

Kwestia definicji

Niestety, pomimo powszechnej popularności tematyki cyberbezpieczeństwa, jego rola i znaczenie jest ciągle niedoceniane i często postrzegane jako zbędne obciążenie, szczególnie w infrastrukturze przemysłowej. Sytuację dodatkowo komplikuje fakt, że związana z tym tematem terminologia jest często źle rozumiana lub niewłaściwie stosowana. Wiele ludzi używa pojęć bezpieczeństwo informacji, bezpieczeństwo komputerowe i cyberbezpieczeństwo zamiennie, podczas gdy dla innych osób każdy z tych terminów ma trochę inne znaczenie. Dla jasności w niniejszym artykule, bezpieczeństwo komputerowe zakłada ochronę wszelkich zasobów cyfrowych, które zawierają, przetwarzają, przesyłają lub przechowują dane elektroniczne, przed szerokim zakresem zagrożeń. Bezpieczeństwo informacji chroni poufność, integralność i dostępność informacji niezależnie od jej formatu. Ponieważ coraz więcej danych jest przechowywanych w formacie cyfrowym, można przyjąć, że bezpieczeństwo informacji i bezpieczeństwo komputerowe to dwie strony tej samej monety i wspólnie nazwać je cyber bezpieczeństwem lub bezpieczeństwem teleinformatycznym.

Nie przewidywano zagrożenia

Jakkolwiek pierwsze komputery pojawiły się na rynku na pod koniec lat 40, cyberbezpieczeństwo zaistniało dopiero na początku lat 70 XX wieku [1]. Działo się to tak dlatego, że przy niewielkiej liczbie komputerów podłączonych do sieci ograniczonych tylko do kilku in-

1) Early Computer Security Papers (1970-1985), National Institute of Standards and Technology, Retrieved from http://csrc.nist.gov/publications/history/index.html

stytucji militarnych i akademickich, cyber bezpieczeństwo było uważane za „problem ludzki". Wstępnie założenia były takie, że jeśli ludzie będą postępować zgodnie z przyjętymi zasadami używania komputerów, zainstalowane na nich systemy operacyjne i programy są wystarczające do zapewnienia ich bezpieczeństwa i bezpieczeństwa przechowywanych na nich danych. W tym okresie, priorytetem dla infrastruktury komputerowej było zapewnienie dostępu i przesyłanie informacji z komputera A do komputera B, a nie ryzyko nieautoryzowanego dostępu, kradzieży lub modyfikacji tych informacji. Przyjęcie takiego podejścia do cyber bezpieczeństwa w tamtym okresie było możliwe tylko ze względu ograniczoną liczbę profesjonalnych i wysoce odpowiedzialnych użytkowników. W miarę jednak jak zasoby komputerowe rosły i dostęp do nich uzyskiwała coraz większa liczba osób, model odpowiedzialnego użytkownika i samokontroli stawał się niewystarczający.

Kruche bezpieczeństwo

Raport opublikowany w 1969 r. przez Willisa Ware z RAND Corporation, zwrócił uwagę Departamentowi Obrony USA na słabości i techniczne ograniczenia istniejących mechanizmów kontroli bezpieczeństwa w ich komputerach i rozpoczął faktyczny rozwój tej dyscypliny[2]. Ponieważ systemy informatyczne prawie od samego początku obejmowały złożone i ciągle zmieniające się technologie, rozwiązania służące ich ochronie musiały praktycznie od samego początku stawiać czoła nieustającemu wyzwaniu, jakim jest nie tylko nadążanie za ich szybkim rozwojem, ale także rosnącą pomysłowością ludzi na wykorzystanie zaistniałych w nich słabości i podatności na cyberataki.

Dużo się zmieniło się od czasu opublikowania raportu RAND. Dawno minęły czasy, gdy największym problemem administratorów systemów informatycznych byli tzw. script kiddie (niedoświadczeni hakerzy), dla których uzyskanie nieuprawnionego dostępu do komputera lub podmienienie zawartości strony internetowej było osiągnięciem zamierzonego celu. Obecnie niemal codziennie słyszymy o cyberatakach na znane organizacje, na skutek których są np. pozyskane przez hakerów poufne dane klientów witryn e-commerce (niestety często nieodpowiednio zabezpieczonych) lub następuje kradzież laptopa rządowej organizacji z wrażliwymi danymi jego personelu. Nawet firmy specjalizujące się w cyberbezpieczeństwie nie są odporne na naruszenia i udane ataki hakerskie.

Początki

Ponieważ początkowo przedmiotem cyberataków były sieci i komputery biurowe, a wraz z rozwojem Internetu serwisy i aplikacje internetowe, spowodowało to, że przez długi czas pokutował pogląd, że instalacje przemysłowe nie tylko nie są przedmiotem zainteresowania hakerów ale także są mało podatne na tego typu ataki. Dodatkowymi argumentami wspierającymi takie przekonania był fakt, że w procesach produkcyjnych są wykorzystywane głównie specjalistyczne systemy sterowania (ICS[3]), w składa których wchodzą lokalne systemy kontroli i gromadzenia danych (SCADA[4]), rozproszone systemy kontroli (DCS[5]) i programowalne sterowniki logiczne (PLC[6]). W przeciwieństwie do biurowych systemów IT opartych na dobrze znanych standardach, większość przemysłowych komputerów powstało w przeszłości z wykorzystaniem zastrzeżonych i chronionych przez producentów technologii oprogramowania i protokołów komunikacyjnych, dla których nie zostały opublikowane szczegółowe specyfikacje. Poza tym, priorytetem ICS zawsze była i jest ich niezawodność, utrzymanie i dostępność (RMA[7]) a nie ich bezpieczeństwo. Ponieważ środki i mechanizmy bezpieczeństwa mogą mieć negatywny wpływ na ich właściwe funkcjonowanie, architektura komponentów ICS prawie nigdy nie miała ich w siebie wbudowanych. W zamian było przyjęte uważać, że odseparowanie tych systemów od sieci komputerowych i fizyczne ograniczenie dostępu do urządzeń przemysłowych jest wystarczającym środkiem bezpieczeństwa przeciwko potencjalnym ale raczej mało prawdopodobnym (jak wtedy uważano) cyberatakom.

Ataki na coraz większą skalę

Stuxnet[8], który pojawił się w latach 2009-2010 łatwo wykazał, że komputery przemysłowe są tak samo podatne na cyber ataki jak komputery biurowe. Wirus ten został wykorzystany między innymi do zaatakowania programowalnych sterowników logicznych (PLC) w obiektach nuklearnych w Iranie gdzie przez ponad rok skutecznie uszkadzał wirówki do produkcji paliwa jądrowego w zakładach wzbogacania uranu w Natanz. Ani specjalistyczne oprogramowanie ani brak połączenia urządzeń przemysłowych z Internetem nie było przeszkodą to zaatakowania tych urządzeń przy pomocy zainfekowanej pamięci podręcznej USB. Innym przykładem cyberataku na instalacje przemysłowe jest wirus BlackEnergy, który w 2015 r. przejął kontrolę nad systemami automatycznego sterowania lokalnymi sieciami energetycznymi w zachodniej Ukrainie i spowodował wyłączenie na kilka godzin dostawy prądu do prawie 1.5 miliona ludzi. W organizacjach przemysłowych przedmiotem cyberataku mogą być oczywiście też komputery

2) Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security - RAND Report R-609-1, RAND Corporation, http://www.rand.org/pubs/reports/R609-1/index2.html

3) Z angielskiego: Industrial Control Systems

4) Z angielskiego: Supervisory Control And Data Acquisition

5) Z angielskiego: Distributed Control Systems

6) Z angielskiego: Programmable Logic Controller

7) Z angielskiego: Reliability, Maintainability, Availability

8) An Unprecedented Look at Stuxnet, the World's First Digital Weapon, Kim Zetter, Wired, 2014, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet

biurowe. Np. w 2012 r. wirus Shamoon[9] został wykorzystany do wykradzenia poufnych informacji z koncernu paliwowo-chemicznego Saudi Aramco w Arabii Saudyjskiej i rafinerii gazowej RasGas w Katarze. W ramach ataku wirus kompilował listę zidentyfikowanych plików, które następnie przesyłał do atakującego systemu, po czym usuwał je z zainfekowanych komputerów. Na koniec wirus uszkadzał sektor rozruchowy dysku aby było niemożliwe ponowne uruchomienie komputera, z których zostały wykradzione informacje. Jak więc widać, organizacje przemysłowe nie tylko są narażone na cyberataki, ale stoją przed podwójnym wyzwaniem, bo muszą chronić zarówno systemy IT jak i systemy ICS, które wymagają innego podejścia ze względu na ich specyficzne wymagania.

Odmienne grupy systemów, odmienne sposoby obrony

Ze względu na dużo niższy popyt i wysoki koszt sprzętu ICS, jest on produkowany na znacznie mniejszą skalę niż komputery biurowe. Dlatego oczekiwania wobec niego są, że będzie działał przez 20-30 lat a czasem i dłużej. Dla wielu przemysłowych systemów zbudowanych dawno temu nie ma po prostu rozwiązań technologicznych typu antywirus czy firewall a nawet gdyby zostały one teraz utworzone, to ich zainstalowanie może być nadal niemożliwe. W przeciwieństwie do tradycyjnych systemów IT łatwo tolerujących częste ponowne uruchamianie oraz pewien poziom opóźnienia spowodowany interakcją z systemem bezpieczeństwa, sprzęt przemysłowy ma zwykle bardzo wysokie wymagania ciągłości operacji i reagowania w czasie rzeczywistym lub zbliżonym do rzeczywistego, bo nawet milisekundowe opóźnienie może wpłynąć negatywnie na proces operacyjny lub spowodować jego awarię. Przeniesienie ich do trybu offline w celu konserwacji i aktualizacji jest często niemożliwe, chyba że równoległy system zapasowy może przejąć kontrolę nad operacjami produkcyjnymi albo taka przerwa jest zaplanowana z odpowiednim wyprzedzeniem. Trzeba jednak pamiętać, że prawie każdy przestój produkcyjny, nawet krótki wiąże się ze stratami finansowymi a utrzymanie w gotowości produkcyjnej zapasowego systemu kontroli i monitorowania to też dodatkowy koszt dla organizacji.

W wielu obiektach przemysłowych, np. takich jak elektrownia atomowa czy zakład chemiczny, niezawodność tych systemów nie może być naruszona, bo konsekwencje awarii mogą być tragiczne w skutkach zarówno dla ludzi jak i dla środowiska. Niewłaściwe zainstalowanie aktualizacji oprogramowania może doprowadzić do zaistnienia większego zagrożenia niż tego, przed którym system miał być chroniony. Dlatego, aby zminimalizować ryzyko takiego wydarzenia, każda planowana zmiana wymaga przed jej wdrożeniem przeprowadzenia ekstensywnych testów dla poszczególnych komponentów ICS (zarówno sprzętu jak i oprogramowania) oraz dla całego systemu. Niezbędne jest też prowadzenie bardzo szczegółowej ewidencji wprowadzanych zmian. Kontrolowane zarządzanie nimi nie tylko utrzymuje ich historię, ale także ułatwia w ich wycofaniu na wypadek gdyby to się okazało konieczne. Przestrzeganie tak rygorystycznego procesu zmian jest bardzo kosztowne i nierzadko jest największą pozycją w budżecie przeznaczonym na konserwację infrastruktury przemysłowej.

Z wyżej wymienionych powodów program cyberbezpieczeństwa w obiektach przemysłowych musi oprzeć się w równym stopniu na następujących elementach modelu bezpieczeństwa: strategia i procedury, element ludzki i technologie. Strategia i procedury pozwalają na długo terminowe zaplanowanie co i kiedy można zrobić oraz kto i w jakim zakresie jest odpowiedzialny za konkretne działania. Większy udział ludzi jest konieczny, bo nie wszędzie da się wdrożyć zautomatyzowane rozwiązania technologiczne. Np. kiedy fizyczne zabezpieczenia mogą być jedyną formą ochrony dla systemów przemysłowych, ich modyfikacje są wykonywane w obecności co najmniej 2 osób. Jedna z nich dokonuje koniecznych zmian, a druga nadzoruje pierwszą aby ich wykonanie nie odbiegało od zaplanowanych działań oraz aby ograniczy do minimum ryzyko popełnienia błędu lub sabotażu. Dla zminimalizowania zagrożenia ze strony człowieka konieczne jest też budowanie w zakładzie przemysłowym kultury bezpieczeństwa, której celem jest wytworzenie wśród pracowników nie tylko odpowiedzialnego zachowania ale też właściwego reagowania na wypadek zauważenia zagrożenia. Przemysłowy program cyberbezpieczeństwa musi też posiadać plan szacowania ryzyka, który powinien ocenić nie tylko pierwotne zagrożenia chronionych systemów, ale także ewentualne ryzyka wtórne, które mogą się zmaterializować w wyniku reakcji na pierwotne ryzyka.

Podsumowując, cyberbezpieczeństwo przemysłowe wymaga dobrej współpracy między ekspertami od systemów komputerowych i tych, którzy zapewniają ochronę całego obiektu. W przemyśle nuklearnym przyjęło się to nazywać planem bezpieczeństwa 4G[10].

□

9) Shamoon virus targets energy sector infrastructure, BBC News, 2012, http://www.bbc.com/news/technology-19293797

10) Gates, Guards, Guns and Geeks