Energetyka 24

09.10.2015

CZY ATAKI CYBERNETYCZNE ZAGROŻĄ POLSKIEMU ATOMOWI?

W dyskusji o bezpieczeństwie infrastruktury związanej z energetyką atomową do coraz częściej poruszanych tematów należą cyberzagrożenia. Wydłuża się zarówno lista potencjalnych podmiotów, mogących wykorzystać działania w cyberprzestrzeni na swoją korzyść, jak i lista możliwych celów ich działania. Również osoby odpowiadające za polską energetykę atomową, na długo przed uruchomieniem siłowni, będą musiały zwrócić uwagę na poziom cyberzabezpieczeń.

W ostatnich dniach w polskich mediach toczyła się dyskusja na temat budowy lub zaniechania prac nad elektrownią atomową. Jej przyczyną stała się kontrowersyjna wypowiedź premier Ewy Kopacz. Jednocześnie, gdy burza polityczno-medialna, ściśle powiązana z kampanią wyborczą, zepchnęła problematykę energii atomowej na tory rywalizacji pomiędzy głównymi partiami politycznymi, na Zachodzie pojawił się bardzo interesujący raport dotykający kluczowego aspektu energetyki atomowej. Jego celem było zaprezentowanie głównych cyberzagrożeń i ich bezpośredniego wpływu na funkcjonowanie wszelkich instalacji atomowych. Autorzy - Caroline Baylon, Roger Brunt i David Livingstone - to przedstawiciele Chatham House, jednego z najbardziej poważanych na świecie think tanków, specjalizującego się m.in. w kwestiach bezpieczeństwa. Na prawie 40 stronach raportu zwrócili oni uwagę na całą gamę zagrożeń i - powiedzmy wprost - wyzwań, przed jakimi staje obecny użytkownik instalacji związanych z energią atomową. Niezależnie od decyzji politycznych już teraz trzeba zastanowić się nad poruszonymi tam problemami, rozpatrując je w kontekście możliwości użytkowania tego rodzaju instalacji w Polsce.

Przede wszystkim należy zauważyć, że inwestując pieniądze w rozwój infrastruktury powiązanej z energią atomową, należy spodziewać się prób uzyskania wpływu na zastosowane tam systemy komputerowe - co do tego raczej nie można mieć żadnych wątpliwości. Polska zdecydowanie nie byłaby tutaj wyjątkiem, a raczej z racji pewnych opóźnień w zakresie wdrażania światowych norm cyberbezpieczeństwa, stanowiłaby idealny cel. Cel, zresztą, nie tylko dla wrogich państw lub aktorów powiązanych z ich instytucjami, ale również terrorystów i zwykłych przestępców. Motywy ich działania mogą być przy tym bardzo różne - od politycznych po zwykłą chęć zysku np. poprzez żądanie okupu. Jednocześnie trzeba zgodzić się z autorami wspomnianego raportu, iż nawet drobny, ale skutecznie nagłośniony incydent, związany z tego rodzaju sektorem energetyki, będzie oddziaływał ze zwiększoną siłą na stosunek społeczeństwa i zapewne polityków do całości problematyki energii atomowej. Dlatego też tak kluczowym wymogiem jest posiadanie odpowiedniego zaplecza w sferze cyberbezpieczeństwa, szczególnie wokół tego rodzaju krytycznej infrastruktury.

W przypadku zabezpieczenia podobnych obiektów na świecie, przez ostatnie lata skupiano uwagę raczej na problemie fizycznej ochrony np. elektrowni atomowych. Starano się zapobiegać choćby możliwości groźby ataku przez grupy terrorystyczne czy infiltracji przez wrogie zespoły dywersyjne, na tym kierunku skupiając większość dostępnych, zaangażowanych w ochronę sił oraz środków. I chociaż również w tym zakresie istnieją pewne niedociągnięcia, to jednak trzeba przyjąć, że na Zachodzie

wypracowano całkiem dobre standardy w zakresie zapewnienia ochrony infrastrukturze atomowej. Tym niemniej obecne „nowe" cyberzagrożenia mogą wydawać się o wiele bardziej niebezpieczne. Przede wszystkim dlatego, że mogą w dużej mierze bazować na nieświadomości i niższej samoświadomości potrzeby zachowania procedur bezpieczeństwa wśród osób zaangażowanych w obsługę tego rodzaju instalacji. Nie może więc zupełnie zaskakiwać, że eksperci z Chatham House, w pierwszej kolejności jako swoisty punkt odniesienia wskazali uderzenie wyprowadzone w irański program atomowy za pomocą złośliwego oprogramowania Stuxnet. To ono chyba w sposób najbardziej brutalny uświadomiło wszystkim, że zagrożenia związane z infrastrukturą komputerową krytycznie istotnych systemów przemysłowych i energetycznych nie są dylematami natury akademickiej, lecz realnymi wyzwaniami.

Użycie Stuxnet jako narzędzia walki z infrastrukturą atomową wykazało dobitnie, że nawet najbardziej wyrafinowane starania, mające na celu wydzielenie systemów komputerowych obsługujących maszynerię instalacji atomowych od ogólnych sieci, podatnych na cyberataki, nigdy nie jest stuprocentowo skuteczne. Pokazało też, że uderzenie tego rodzaju może być skuteczne i spowodować gigantyczne straty w skomplikowanym i kosztochłonnym programie atomowym, nawet takim, który pozostawał mało przejrzysty dla świata. Irańczycy doskonale zdawali sobie sprawę z możliwości przeprowadzenia ataku cybernetycznego na prowadzony przez nich program, choćby w związku z oskarżeniami wspólnoty międzynarodowej oraz - najpewniej - bezpośrednimi działaniami Izraela, dla którego nuklearny Iran był jednym ze strategicznych wyzwań. Dlatego niewątpliwie starali się podejmować jak największe środki ostrożności, aby minimalizować możliwość działania hakerów chociażby izraelskich czy amerykańskich, działających na zlecenie tamtejszych władz.

Dlatego, jeśli udało się skutecznie zaatakować Irańczyków, rodzi się pytanie, które postawiono w raporcie, odnośnie podatności infrastruktury atomowej w państwach mniej nastawionych na ścisłą ochronę swoich systemów obsługujących programy atomowe. Jest to szczególnie istotne również dlatego, że współcześnie bardzo wielu użytkowników energii atomowej dąży do ograniczenia kosztów eksploatacji swoich elektrowni. Pojawiają się pomysły dotyczące pozyskiwanie pewnych podzespołów i oprogramowania na otwartym rynku technologii cywilnych, który jest idealnym miejscem rozpoczęcia potencjalnej infiltracji lub ataków na infrastrukturę związaną z energetyką atomową. Trzeba jednak przyznać, że - jak pokazuje sytuacja z Projektem Manhattan w Stanach Zjednoczonych, jeszcze przed erą komputerów - nie ma zabezpieczeń nie do obejścia. W końcu nawet zamknięcie w odludnym miejscu naukowców, pod ścisłą kontrolą wojska i jego kontrwywiadu, nie zapewni nigdy pełnego bezpieczeństwa chociażby w zakresie niekontrolowanego wydostawania się informacji na zewnątrz. Co dopiero w epoce, gdy przenośne dyski, które mogą stać się skutecznym narzędziem walki lub szpiegostwa, stają się tak małe, że niemal niewidoczne.

Wracając do rozważań ekspertów z Chatham House, trzeba podkreślić, że chociaż Stuxnet wyznaczył w pewnym sensie nowe podejście do omawianej problematyki, to z mniej znanymi incydentami mieliśmy do czynienia na całym świecie na długo przed uderzeniem w irańską infrastrukturę. W 1992 r. w ignalińskiej elektrowni atomowej technik z premedytacją wprowadził do systemu kontroli wirusa. W 2003 r. do sieci używanej do zarządzania elektrownią atomową Davis-Besse w Ohio trafił robak określany jako Slammer/W32/SQLSlam-A/Sapphire. Na szczęście reaktor wówczas nie działał, gdyż inaczej mogłoby dojść do zaburzeń w obrębie używanego tam systemu SPDS służącego do prezentacji pomiarów sytuacji wokół rdzenia reaktora czy też poziomów radiacji w całej elektrowni. Rok temu głośny stał się przypadek Korea Hydro and Nuclear Power Co. z Korei Południowej, która padła ofiarą ataku hakerów. Odnosząc się do Stuxnet, słynny na całym świecie Eugene Kaspersky stwierdził, iż to złośliwe oprogramowanie według jego informacji nie zaatakowało tylko irańskich instalacji, ale pojawiło się również w jednej nieokreślonej lokacji w Rosji. Oczywiście, pojawia się pytanie czy było to działanie z premedytacją, czy jedynie odprysk działań wymierzonych w Iran. Tym niemniej i z taką ewentualnością należy liczyć się w każdym z państw korzystających z technologii atomowej. W końcu

część rozwiązań i architektury sieci stosowanych na całym świecie ma wspólne elementy, a więc jest w dużej mierze podatna na włamania czy też ataki różnych podmiotów z wykorzystaniem analogicznych narzędzi, np. złośliwego oprogramowania.

Trzeba uzmysłowić sobie, że sama izolacja infrastruktury związanej z energetyką atomową jest dziś nie tyle, że niemożliwa, co również niewystarczająca jako jedyna forma obrony. Hakerzy mogą przecież spokojnie wykorzystać luki w zakresie komercyjnych sieci firm zaangażowanych w obsługę infrastruktury, a także wykorzystywać błędy lub celowe omijanie standardów bezpieczeństwa przez pracowników. Zawsze istnieje też zagrożenie atakiem od wewnątrz. W końcu zdarzyć się może też sytuacja, w której ktoś zechce zaatakować systemu obsługujące infrastrukturę cybernetyczną nie tyle przez swoją nieuwagę lub zaniedbanie, a z premedytacją. Wątpliwa jest też sama izolacja, szczególnie jeśli zauważy się tendencję do rosnącego nacisku na szybki transfer danych i wymianę informacji pomiędzy różnymi elementami infrastruktury energetycznej. W końcu przypadkowy dysk USB, czy jakiś nośnik danych ze sterownikami zawsze może trafić do odizolowanej sieci, wnosząc do niej niechciane oprogramowanie.

Wobec powyższego niezwykłej wagi nabiera synergia wielu czynników wpływających na cyberbezpieczenstwo, nie ograniczanie się do jedynie specjalistycznego oprogramowania (firewalli, programów szyfrujących, antywirusowych zabezpieczeń w obrębie wewnętrznych sieci itp.). Trzeba bowiem wypracować odpowiednie kanały przekazu informacji pomiędzy różnymi podmiotami nie tylko krajowymi, ale międzynarodowymi, które mogą wspólnie wymieniać się doświadczeniami. Najgorsze, co zdaniem ekspertów może przydarzyć się w dziedzinie cyberbezpieczeństwa takich obiektów, to ukrywanie incydentów - ułatwia to atakowanie infrastruktury w innych miejscach z użyciem podobnych narzędzi. Nie ma też rozróżnienia na różne części gospodarki, czy podmioty w przemyśle kontrolowanym przez państwo lub pozostające w prywatnych rękach. Konieczne jest też umiejętne kontrolowanie dostawców i podwykonawców, główni operatorzy i producenci najważniejszych podzespołów oraz oprogramowania w sferze energii atomowej starają się sami zachowywać najwyższe standardy bezpieczeństwa. Nie zawsze da się powiedzieć to samo o mniejszych partnerach, a przecież zagrożenie płynące z ich strony, a wynikające z ewentualnych zaniedbań, może być równie niebezpieczne dla całości inwestycji.

Jeśli chodzi o powinności państwa, to jeszcze przed fizycznym powstaniem jakiejkolwiek infrastruktury należy podjąć całe spektrum działań zabezpieczających. Od wspomnianej ścisłej kontroli wywiadowczej/kontrwywiadowczej nad samą technologią, jej wykonawcami i podwykonawcami w danym projekcie, aż po wzmocnienie sił oraz potencjału CERT ABW. Ważne jest też wprowadzenie pewnej standaryzacji poziomu cyberzabezpieczeń na szczeblu państwa, można przy tym korzystać chociażby z doświadczeń innych, zaprzyjaźnionych państw. Państwo powinno również naciskać w zdecydowany sposób na operatorów w celu wspierania projektów szkoleniowych dla osób pracujących przy energetyce atomowej, edukowanych z myślą o najgorszych scenariuszach, a więc pod uwagę trzeba brać nie tylko możliwość wystąpienia incydentów mniejszej wagi. lecz również zagrożenia wymagającego pełnoskalowego reagowania kryzysowego w sferze cyberbezpieczeństwa. Bądź co bądź, jeśli chcielibyśmy myśleć o budowie energetyki atomowej, to należy zrównać bezpieczeństwo konwencjonalne infrastruktury oraz cyberbezpieczeństwo, nie wolno powtarzać nam dotychczasowych złych tendencji, uwidocznionych w raporcie, a dotyczących niektórych państw zachodnich.

Podsumowując, jakakolwiek inwestycja w energię atomową w Polsce musi być połączona z inwestycją w poprawę poziomu cyberbezpieczeństwa w kraju. Jednocześnie nie można jednoznacznie stwierdzić, że nawet największe wstępne wydatki na zabezpieczenia pozwolą na pełne zabezpieczenie infrastruktury w ciągu kolejnych lat. Cyberzagrożenia są bowiem coraz większym wyzwaniem dla użytkowników energii atomowej, a w przyszłości mogą nawet stać się głównym wyzwaniem, przed jakim staną podmioty prywatne oraz publiczne. Dlatego potencjalna inwestycja w elektrownię atomową powinna być inwestycją w polskie firmy, zajmujące się cyberbezpieczeństwem i okazją do

wzmocnienia instytucji publicznych stojących w pierwszej linii walki z hakerami i szpiegostwem bazującym na wykorzystaniu sieci teleinformatycznych. Warto również już teraz dokładnie monitorować wszelkie pojawiające się na całym świecie raporty oraz analizy, jak chociażby omawiana analiza z Chatham House. Konieczne jest nie tylko wczytywanie się w powielane w mediach skróty, lecz dokładne rozważenie wszelkich opisanych tam przypadków i ich analiza pod kątem możliwych zaleceń i rekomendacji dla polskich operatorów potencjalnej infrastruktury atomowej.

Zobacz także: Bez atomu Polsce może grozić „energetyczny kolonializm”

Zobacz także: Wicepremier Piechociński: musimy wybudować elektrownię atomową