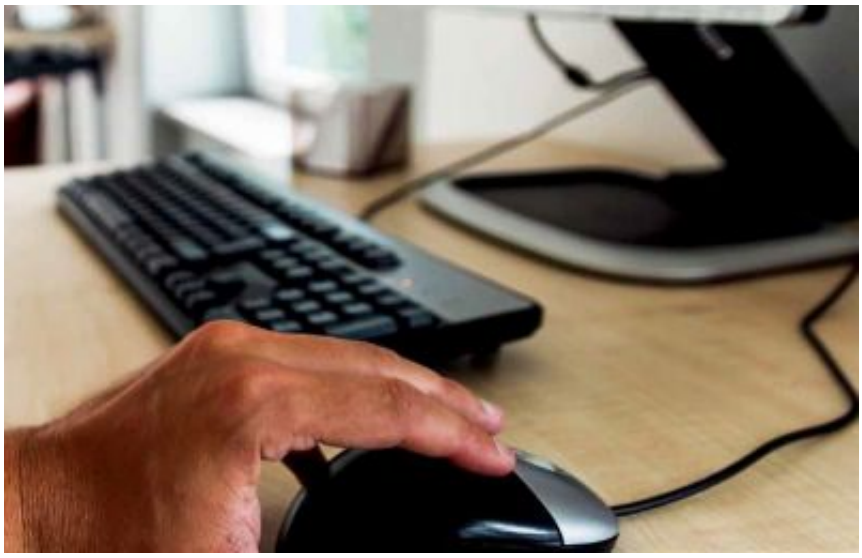
Wiadomości

2016-03-17

Polska energetyka a cyberataki - komentuje Bożenna Piątkowska, Wyższa Szkoła Bezpieczeństwa w Gdańsku



Skutki ataku informatycznego w sektorze energetycznym stają się tym większe, im bardziej ogranicza się wydatki na zabezpieczenia, infrastrukturę krytyczną oraz systemy sterowania przemysłowego. Potrzebne są zintegrowane działania sektorów publicznego i prywatnego. Bezpieczeństwo cyberprzestrzeni to bowiem kwestia bezpieczeństwa narodowego.

Rosnące zagrożenie infrastruktury krytycznej państwa stanowią zwłaszcza zdalne włamania do sieci informatycznych (tzw. cyberataki) dokonywane przez zorganizowane grupy hakerów (ang. *hacker* – dosł.: łamacz; tu łamacz zabezpieczeń informatycznych, włamywacz)[1]. Sektor energetyczny jest zagrożony w stopniu szczególnym ze względu na automatyzację tej branży oraz bieżącą konieczność wprowadzania nowych systemów kontrolujących wydobycie i dystrybucję ropy oraz gazu. Początkowo cyberataki były motywowane finansowo, a domorośli hakerzy sprawdzali tylko swe umiejętności. Z czasem zjawisko to przyjęło formę przestępczości zorganizowanej. [...]

WIĘCEJ: czytaj w marcowym wydaniu miesięcznika „Paliwa Płynne”

Jeżeli zależy Ci na bezpieczeństwie energetycznym Polski, odwiedź koniecznie XXIII Międzynarodowe Targi STACJA PALIW 2016, 11-13 maja 2016 r. EXPO XXI Warszawa

W 2014 r. firma iSight Partners ujawniła, iż grupa hakerów rosyjskich szpiegowała m.in. jedną z polskich firm z branży energetycznej[1]. W tym samym roku Symantec Corporation[2] poinformowała, że grupa hakerów o nazwie Dragonfly[3] prowadziła od 2013 r. ataki na firmy z sektora energetycznego, w tym w Polsce – ich celem mieli być m.in. producenci energii i rurociągów[4]. Co prawda ograniczyli się do szpiegostwa, ale gdyby doszło do sabotażu, byłyby nieodwracalne. Optymizmem nie napawa *Raport o*

stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL[5], pełniący rolę głównego zespołu CERT i odpowiadający za koordynację procesu reagowania na incydenty komputerowe w obszarze administracji rządowej, podał w nim, że 2014 r. był rekordowy. Zarejestrowano 12017 zgłoszeń, z których 7498 zakwalifikowano jako incydent[6]. Dla porównania w 2013 r. incydentów było 5670, w 2012 r. 457, 2011 r. 249[7]. Celami ataków były firmy: energetyczne, sektora zbrojeniowego, IT oraz agencje rządowe[8]. Raport podkreśla, że z uwagi na dostępność i łatwość korzystania z internetu i mediów społecznościowych są one narzędziem stosowanym do akcji militarnych i wywiadowczych prowadzonych przez państwa.[...]

WIĘCEJ: czytaj w marcowym wydaniu miesięcznika „Paliwa Płynne”

Jeżeli zależy Ci na bezpieczeństwie energetycznym Polski, odwiedź koniecznie XXIII Międzynarodowe Targi STACJA PALIW 2016, 11-13 maja 2016 r. EXPO XXI Warszawa

W 2011 r. do polskiego systemu prawnego wprowadzono pojęcie „cyberprzestrzeni”. Opracowano *Politykę Ochrony Cyberprzestrzeni RP*[1], dokument, który 25 czerwca 2013 r. w drodze uchwały przyjęła Rada Ministrów. We wstępie czytamy, że celem strategicznym jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Ma to być realizowane poprzez ramy organizacyjno-prawne, a także system koordynacji i wymiany informacji między użytkownikami CRP (mowa o cyberprzestrzeni RP)[2].[...]

WIĘCEJ: czytaj w marcowym wydaniu miesięcznika „Paliwa Płynne”

Jeżeli zależy Ci na bezpieczeństwie energetycznym Polski, odwiedź koniecznie XXIII Międzynarodowe Targi STACJA PALIW 2016, 11-13 maja 2016 r. EXPO XXI Warszawa

W raporcie założono, iż ważnym elementem jest współpraca z przedsiębiorcami, w szczególności w sektorach: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowym oraz transportowym.[...]

Podsumowując, modernizacja i przebudowa struktury energetycznej jest na etapie początkowym. Przedstawione wcześniej wydarzenia związane z cyberatakami pokazują, że zagrożenie jest duże i bardzo realne. Energetyka, z uwagi na strategiczne znaczenie dla bezpieczeństwa państwa, jest coraz częściej kluczowym celem cyberprzestępców o zorganizowanej i sterowalnej strukturze. Tymczasem w Polsce bezpieczeństwo w cyberprzestrzeni nie jest właściwie chronione. Z „Informacji o wynikach kontroli” NIK z 23 czerwca 2015 r. wynika, iż bezpieczeństwo teleinformatyczne w naszym kraju pozostaje na bardzo niskim poziomie[1]. Podmioty państwowe związane z ochroną cyberprzestrzeni, prowadziły działania z tego zakresu w sposób rozproszony i bez spójnej wizji systemowej. Działania tych podmiotów były jedynie doraźne, a reagowanie na bieżące wydarzenia było zdecydowanie ograniczone. Poważnym problemem, na co podkreślali eksperci NIK, było brak właściwych i niezbędnych rozwiązań legislacyjnych, przez co nie unormowano kwestii związanych z bezpieczeństwem w cyberprzestrzeni.

Jedno jest pewne, że wrażliwość infrastruktury energetycznej na cyberataki będzie na przestrzeni lat rosła.

[1]Zob. szerzej, *Informacja o wynikach kontroli Realizacja przez podmioty państwowe zadań w zakresie cyberprzestrzeni RP*, 23.06.2015 r., http://www.nik.gov.pl/plik/id,8764,vp,10895.pdf,22.11.2015 r.

[1] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej,* 25.06.2013 r., http://www.cert.gov.pl/cer/publikacje/polityka-chrona-..., (pobrano 22.12.2015 r.). Dokument opracowano w Ministerstwie Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego

[2]Ibidem, s. 6

[1] Zob. szerzej, *Rosyjscy hakerzy szpiegowali polską firmę, 14.10.2014 r.*. http://www.bankier .pl/wiadomosc/Rosyjscy-hakerzy-szpiegowali-polska-firme-32181, 19.12.2015 r.

[2] Firma Symantec Coropration została założona w 1982 r. i jest międzynarodowym przedsiębiorstwem koncentrującym się szczególnie w dziedzinie bezpieczeństwa danych i zarządzania informacjami.

[3] Dragonfly to dobrze zorganizowana grupa hackerska, znana również pod nazwą „Energetic Bear" – jej działania wymierzone są w szereg firm, w tym przede wszystkim z sektora energetycznego. Do głównych krajów będących w zainteresowaniu grupy należą: Stany Zjednoczone, Hiszpania, Francja, Włochy, Niemcy, Turcja oraz Polska.

[4] Zob. szerzej, *Branża energetyczna celem szpiegostwa cybernetycznego,* 19.10.2014 *r.,* http://www. Polityce.pl/gospodarka/218655-branza-energetyczna-celem-szpiegostwa-cyberne…, 19.12.2015 r.

[5] Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL powołano 1 lutego 2008 r., działający w ramach Agencji Bezpieczeństwa Wewnętrznego. Podstawowym zadaniem zespołu jest zapewnienie i rozwijanie zdolności jednostek organizacji administracji publicznej RP do ochrony przez cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić m.in. zagrożenie dla życia, zdrowia ludzi i funkcjonowania państwa

[6] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014,* http://www.cert.gov.pl/../RaportostaniebezpieczenstwacyberprzestrzeniRPw2014r..., s. 6 (pobrano 22.11.2015 r.)

[7] Zob. *Raporty o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2013, 2012 i 2011,* http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-..., 19.12.2015 r.

[8] *Raport …w roku 2014,* op. cit., s. 17

[1] *Raport Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny,* s. 16, http://www.ik.org.pl/cms/wp-content/.../RAPORT_Infrastruktura-krytyczna_net.pdf, 22.11.2015 r. Raport przygotował Instytut Kościuszki wraz z partnerami. W dokumencie zapisano, iż infrastrukturę krytyczną (IK) można pogrupować na: - zapewniającą schronienie i prawidłowe jego funkcjonowanie (są to najczęściej np. ciepłownie, elektrownie); - infrastrukturę zabezpieczającą (np. infrastruktura drogowa, wodociągowa, rafinerie); - infrastruktura dostarczająca usługi (np. centrale telefoniczne, elektrownie, rafinerie, bazy danych). Na temat infrastruktury krytycznej zob. art. 3 ust. ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, tekst jednolity - Dz. U. z 2013 r. poz. 1166, z późn. zm.

Źródło:
http://paliwa.pl/strona-startowa/archiwum/polska-energetyka-a-cyberataki-komentuje-bozenna-piatkowska-wyzsza-szkola-bezpieczenstwa-w-gdansku