ZALECENIA

ZALECENIE KOMISJI (UE) 2019/553

z dnia 3 kwietnia 2019 r.

w sprawie cyberbezpieczeństwa w sektorze energetycznym

(notyfikowana jako dokument nr C(2019) 2400)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

a także mając na uwadze, co następuje:

(1) Europejski sektor energetyczny przechodzi istotną zmianę w kierunku gospodarki niskoemisyjnej, przy jednoczesnym zapewnieniu bezpieczeństwa dostaw i konkurencyjności. W ramach tej transformacji energetycznej i związanej z nią decentralizacji wytwarzania energii elektrycznej ze źródeł odnawialnych, postęp technologiczny, łączenie sektorów i cyfryzacja przekształcają europejską sieć energetyczną w „inteligentną sieć". Jednocześnie niesie to ze sobą nowe zagrożenia, ponieważ cyfryzacja w coraz większym stopniu naraża system energetyczny na cyberataki i incydenty, które mogą zagrażać bezpieczeństwu dostaw energii.

(2) Przyjęcie wszystkich ośmiu wniosków ustawodawczych ([1]) dotyczących pakietu „Czysta energia dla wszystkich Europejczyków", w tym zarządzania unią energetyczną jako etapu wstępnego, umożliwia stworzenie środowiska sprzyjającego transformacji cyfrowej w sektorze energetycznym. Uznaje się również w jego ramach znaczenie cyberbezpieczeństwa w sektorze energetycznym. W szczególności wersja przekształcona rozporządzenia w sprawie wewnętrznego rynku energii elektrycznej ([2]) przewiduje przyjęcie przepisów technicznych dotyczących energii elektrycznej, takich jak kodeks sieci dotyczący sektorowych przepisów w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej, wspólnych minimalnych wymogów, planowania, monitorowania, sprawozdawczości i zarządzania kryzysowego. Rozporządzenie w sprawie gotowości na wypadek zagrożeń w sektorze energii elektrycznej ([3]) jest zasadniczo zgodne z podejściem przyjętym w rozporządzeniu dotyczącym bezpieczeństwa dostaw gazu ([4]); podkreślając potrzebę właściwej oceny wszystkich zagrożeń, w tym zagrożeń związanych z cyberbezpieczeństwem, oraz proponując przyjęcie środków mających na celu zapobieganie zidentyfikowanym zagrożeniom i ich ograniczanie.

(3) Kiedy w 2013 r. Komisja przyjęła strategię Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego ([5]), jako priorytet wskazała wzmocnienie cyberodporności Unii. Jednym z kluczowych rezultatów strategii jest dyrektywa w sprawie bezpieczeństwa sieci i systemów informatycznych ([6]) (zwana dalej „dyrektywą w sprawie bezpieczeństwa sieci i informacji"), którą przyjęto w lipcu 2016 r. Jako pierwszy element horyzontalnych przepisów Unii w sprawie cyberbezpieczeństwa, dyrektywa w sprawie bezpieczeństwa sieci i informacji zwiększa ogólny poziom cyberbezpieczeństwa w UE, rozwijając krajowe zdolności w zakresie cyberbezpieczeństwa, zwiększając współpracę na szczeblu UE oraz wprowadzając obowiązki w zakresie bezpieczeństwa i zgłaszania incydentów dotyczące przedsiębiorstw zwanych „operatorami usług kluczowych". Zgłaszanie incydentów jest obowiązkowe w kluczowych sektorach, w tym w sektorze energetycznym.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/2001 z dnia 11 grudnia 2018 r. w sprawie promowania stosowania energii ze źródeł odnawialnych (Dz.U. L 328 z 21.12.2018, s. 82); dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/2002 z dnia 11 grudnia 2018 r. zmieniająca dyrektywę 2012/27/UE w sprawie efektywności energetycznej (Dz.U. L 328 z 21.12.2018, s. 210); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1999 z dnia 11 grudnia 2018 r. w sprawie zarządzania unią energetyczną i działaniami w dziedzinie klimatu, zmiany rozporządzeń Parlamentu Europejskiego i Rady (WE) nr 663/2009 i (WE) nr 715/2009, dyrektyw Parlamentu Europejskiego i Rady 94/22/WE, 98/70/WE, 2009/31/WE, 2009/73/WE, 2010/31/UE, 2012/27/UE i 2013/30/UE, dyrektyw Rady 2009/119/WE i (UE) 2015/652 oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 525/2013 (Dz.U. L 328 z 21.12.2018, s. 1); dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/844 z dnia 30 maja 2018 r. zmieniająca dyrektywę 2010/31/UE w sprawie charakterystyki energetycznej budynków i dyrektywę 2012/27/UE w sprawie efektywności energetycznej (Dz.U. L 156 z 19.6.2018, s. 75). Parlament Europejski potwierdził porozumienia polityczne z Radą w sprawie wniosków dotyczących struktury rynku energii elektrycznej (rozporządzenie w sprawie gotowości na wypadek zagrożeń, rozporządzenie w sprawie Agencji ds. Współpracy Organów Regulacji Energetyki (ACER) oraz dyrektywa w sprawie energii elektrycznej i rozporządzenie w sprawie energii elektrycznej) na sesji plenarnej w marcu 2019 r. Formalne przyjęcie przez Radę ma nastąpić w kwietniu; publikacja tekstu prawnego w Dz.U. nastąpi wkrótce potem.

([2]) COM(2016) 861 final.

([3]) COM(2016) 862 final.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1938 z dnia 25 października 2017 r. dotyczące środków zapewniających bezpieczeństwo dostaw gazu ziemnego i uchylające rozporządzenie (UE) nr 994/2010 (Dz.U. L 280 z 28.10.2017, s. 1).

([5]) JOIN(2013) 1.

([6]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

(4) Wdrażając środki gotowości w dziedzinie cyberbezpieczeństwa, odpowiednie zainteresowane strony, w tym operatorzy usług kluczowych w zakresie energii określeni na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji, powinny uwzględniać horyzontalne wytyczne wydane przez grupę współpracy ds. bezpieczeństwa sieci i informacji ustanowioną na mocy art. 11 dyrektywy w sprawie bezpieczeństwa sieci i informacji. Ta grupa współpracy, w skład której wchodzą przedstawiciele państw członkowskich, Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i Komisji, przyjęła wytyczne dotyczące środków bezpieczeństwa i zgłaszania incydentów. W czerwcu 2018 r. grupa ta utworzyła specjalny obszar interwencji dotyczący energii.

(5) We wspólnym komunikacie w sprawie bezpieczeństwa cybernetycznego z 2017 r. ([7]) uznano znaczenie względów i wymogów specyficznych dla danego sektora na szczeblu UE, w tym w sektorze energetycznym. Cyberbezpieczeństwo i ewentualne implikacje polityczne były w ostatnich latach przedmiotem szeroko zakrojonego procesu dyskusji na forum Unii. W związku z tym obecnie rośnie świadomość, że poszczególne sektory gospodarki stoją w obliczu szczególnych problemów związanych z cyberbezpieczeństwem i w związku z tym muszą opracować własne podejścia sektorowe w szerszym kontekście ogólnych strategii cyberbezpieczeństwa.

(6) Wymiana informacji i zaufanie są kluczowymi elementami w dziedzinie cyberbezpieczeństwa. Celem Komisji jest zwiększenie wymiany informacji między odpowiednimi zainteresowanymi stronami poprzez organizowanie specjalnych wydarzeń, takich jak przykładowo forum wysokiego szczebla poświęcone cyberbezpieczeństwu w dziedzinie energii zorganizowane w Rzymie w marcu 2017 r. oraz konferencja wysokiego szczebla w sprawie cyberbezpieczeństwa w dziedzinie energii zorganizowana w Brukseli w październiku 2018 r. Komisja pragnie również zacieśnić współpracę między odpowiednimi zainteresowanymi stronami i wyspecjalizowanymi podmiotami, takimi jak europejski ośrodek wymiany i analizy informacji w sektorze energetycznym.

(7) Rozporządzenie w sprawie Agencji UE ds. Cyberbezpieczeństwa (ENISA) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („rozporządzenie o cyberbezpieczeństwie") ([8]) wzmocni mandat Agencji Unii Europejskiej ds. Cyberbezpieczeństwa w celu lepszego wspierania państw członkowskich w zwalczaniu zagrożeń dla cyberbezpieczeństwa i cyberataków. Tworzą one także europejskie ramy certyfikacji cyberbezpieczeństwa produktów, procesów i usług, które będą ważne w całej Unii i mają szczególne znaczenie dla sektora energetycznego.

(8) Komisja przedstawiła zalecenie ([9]) dotyczące zagrożeń dla cyberbezpieczeństwa w technologiach sieciowych piątej generacji (5G), określając wytyczne na temat odpowiednich krajowych środków w zakresie analizy ryzyka i zarządzania ryzykiem, opracowania skoordynowanej analizy ryzyka na poziomie europejskim oraz ustanowienia procesu opracowywania wspólnego zestawu narzędzi obejmujących najlepsze środki zarządzania ryzykiem. Sieci 5G, po ich wprowadzeniu, będą tworzyły podstawę dla szerokiej gamy usług niezbędnych do funkcjonowania rynku wewnętrznego i działania funkcji mających zasadnicze znaczenie dla społeczeństwa i gospodarki, takich jak energia.

(9) Niniejsze zalecenie powinno zawierać ogólne wytyczne dla państw członkowskich i odpowiednich zainteresowanych stron, w szczególności operatorów sieci i dostawców technologii, dotyczące osiągnięcia wyższego poziomu cyberbezpieczeństwa ze względu na szczególne wymogi czasu rzeczywistego określone dla sektora energetycznego, efekty kaskadowe oraz połączenie dotychczasowych i najnowocześniejszych technologii. Wspomniane wytyczne mają pomóc zainteresowanym stronom w uwzględnianiu szczególnych wymogów sektora energetycznego przy wdrażaniu uznanych na szczeblu międzynarodowym norm dotyczących cyberbezpieczeństwa ([10]).

(10) Komisja zamierza regularnie dokonywać przeglądu niniejszego zalecenia w oparciu o postępy poczynione w całej Unii w porozumieniu z państwami członkowskimi i odpowiednimi zainteresowanymi stronami. Komisja będzie kontynuować wysiłki na rzecz wzmocnienia cyberbezpieczeństwa w sektorze energetycznym, w szczególności poprzez grupę współpracy ds. bezpieczeństwa sieci i informacji, która zapewnia strategiczną współpracę i wymianę informacji między państwami członkowskimi w dziedzinie cyberbezpieczeństwa,

PRZYJMUJE NINIEJSZE ZALECENIE:

PRZEDMIOT ZALECENIA

1. W niniejszym zaleceniu określono główne kwestie związane z cyberbezpieczeństwem w sektorze energetycznym (wymogi czasu rzeczywistego, efekty kaskadowe i połączenie dotychczasowej i najnowocześniejszej technologii) oraz określono główne działania mające na celu wdrożenie odpowiednich środków w zakresie gotowości w dziedzinie cyberbezpieczeństwa w sektorze energetycznym.

([7]) JOIN(2017) 450.

([8]) Akt ws. cyberbezpieczeństwa został przyjęty przez Parlament Europejski w marcu 2019 r. Formalne przyjęcie przez Radę ma nastąpić w kwietniu; publikacja tekstu prawnego w Dz.U. nastąpi wkrótce potem.

([9]) C(2019) 2335.

([10]) Międzynarodowe organizacje normalizacyjne opublikowały różne normy dotyczące cyberbezpieczeństwa (ISO/IEC 27000: Technologie informacyjne) i zarządzania ryzykiem (ISO/IEC31000: Wdrażanie zarządzania ryzykiem). Szczegółową normę dla sektora energetycznego (ISO/IEC 27019: Kontrole bezpieczeństwa informacji dla przemysłu energetycznego) wydano w ramach serii ISO/IEC 27000 w październiku 2017 r.

2. Stosując to zalecenie, państwa członkowskie powinny zachęcać odpowiednie zainteresowane strony do poszerzania wiedzy i umiejętności związanych z cyberbezpieczeństwem w sektorze energetycznym. W stosownych przypadkach państwa członkowskie powinny również uwzględnić te kwestie w swoich krajowych ramach dotyczących cyberbezpieczeństwa, w szczególności poprzez strategie, przepisy ustawowe, wykonawcze i inne przepisy administracyjne.

WYMOGI CZASU RZECZYWISTEGO DOTYCZĄCE ELEMENTÓW INFRASTRUKTURY ENERGETYCZNEJ

3. Państwa członkowskie powinny zapewnić, aby odpowiednie zainteresowane strony, w szczególności operatorzy sieci energetycznych i dostawcy technologii, a zwłaszcza operatorzy usług kluczowych określeni na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji, wdrażały odpowiednie środki w zakresie gotowości związane z cyberbezpieczeństwem odnoszące się do wymogów czasu rzeczywistego w sektorze energetycznym. Niektóre elementy systemu energetycznego muszą funkcjonować w „czasie rzeczywistym", tj. reagując na polecenia w ciągu kilku milisekund, co utrudnia lub wręcz uniemożliwia wprowadzenie środków z zakresu cyberbezpieczeństwa ze względu na brak czasu.

4. W szczególności operatorzy sieci energetycznych powinni:

   a) stosować najnowsze normy bezpieczeństwa w odniesieniu do nowych instalacji wszędzie tam, gdzie jest to właściwe, oraz rozważyć uzupełniające środki bezpieczeństwa fizycznego, w przypadku gdy zainstalowana baza starych instalacji nie może być wystarczająco chroniona przez mechanizmy cyberbezpieczeństwa;

   b) wdrożyć międzynarodowe normy w zakresie cyberbezpieczeństwa i odpowiednie szczegółowe normy techniczne w zakresie bezpiecznej komunikacji w czasie rzeczywistym, gdy tylko odpowiednie produkty staną się dostępne na rynku;

   c) uwzględnić ograniczenia czasu rzeczywistego w ogólnej koncepcji bezpieczeństwa w odniesieniu do aktywów, zwłaszcza w odniesieniu do klasyfikacji aktywów;

   d) wziąć pod uwagę sieci prywatne na potrzeby systemów teleochrony w celu zapewnienia poziomu jakości usług wymaganego w odniesieniu do ograniczeń czasu rzeczywistego. Korzystając z publicznych sieci łączności, operatorzy powinni rozważyć zapewnienie przyznania specjalnej szerokości pasma, wymogów w zakresie opóźnienia i środków bezpieczeństwa w zakresie komunikacji;

   e) podzielić cały system na strefy logiczne i w obrębie każdej strefy określić ograniczenia czasowe i procesowe w celu umożliwienia stosowania odpowiednich środków cyberbezpieczeństwa lub uwzględnienia alternatywnych metod ochrony.

5. O ile to możliwe, operatorzy sieci energetycznych powinni również:

   a) wybrać bezpieczny protokół komunikacyjny uwzględniający wymogi czasu rzeczywistego, np. pomiędzy instalacją a jej systemami zarządzania (system zarządzania energią – system zarządzania dystrybucją);

   b) wprowadzić odpowiedni mechanizm uwierzytelniania dla łączności maszyna-maszyna uwzględniający wymogi czasu rzeczywistego.

EFEKTY KASKADOWE

6. Państwa członkowskie powinny zapewnić, aby odpowiednie zainteresowane strony, w szczególności operatorzy sieci energetycznych i dostawcy technologii, a zwłaszcza operatorzy usług kluczowych określeni na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji, wdrażały odpowiednie środki w zakresie gotowości związane z cyberbezpieczeństwem odnoszące się do efektów kaskadowych w sektorze energetycznym. Sieci elektroenergetyczne i gazociągi są silnie ze sobą połączone w całej Europie, a cyberatak prowadzący do wyłączeń lub zakłóceń w części systemu energetycznego może spowodować daleko idące efekty kaskadowe w innych częściach tego systemu.

7. Stosując niniejsze zalecenie, państwa członkowskie powinny dokonać oceny współzależności i krytyczności systemów wytwarzania energii i elastycznego popytu, podstacji i linii przesyłowych i dystrybucyjnych, a także powiązanych zainteresowanych stron, które odczują skutki (z uwzględnieniem sytuacji transgranicznych) w przypadku skutecznego cyberataku lub cyberincydentu. Państwa członkowskie powinny również zapewnić, aby operatorzy sieci energetycznych dysponowali ramami komunikacyjnymi ze wszystkimi kluczowymi zainteresowanymi stronami w celu wymiany sygnałów wczesnego ostrzegania i współpracy w zakresie zarządzania kryzysowego. Powinny istnieć usystematyzowane kanały komunikacji i uzgodnione formaty w celu wymiany informacji szczególnie chronionych ze wszystkimi zainteresowanymi stronami, zespołami reagowania na incydenty bezpieczeństwa komputerowego oraz właściwymi organami.

8. W szczególności operatorzy sieci energetycznych powinni:

   a) zapewnić, aby nowe urządzenia, w tym urządzenia internetu rzeczy posiadały i utrzymywały poziom cyberbezpieczeństwa odpowiedni do krytyczności danego obiektu;

   b) odpowiednio uwzględnić skutki cyberfizyczne przy ustanawianiu i okresowym przeglądzie planów ciągłości działania;

c) ustanowić kryteria projektowe i architekturę na potrzeby odpornej sieci, co można by osiągnąć poprzez:

— wprowadzenie w każdym obiekcie środków ochrony w głąb dostosowanych do krytyczności danego obiektu,

— identyfikację węzłów krytycznych, zarówno pod względem zdolności wytwórczych, jak i wpływu na klienta. Funkcje krytyczne sieci powinny być zaprojektowane w taki sposób, aby poprzez rozważenie redundancji, odporności na wahania fazy i ochrony przed kaskadowymi wyłączeniami mocy ograniczyć ryzyko, które może wywołać efekty kaskadowe,

— współpracę z innymi właściwymi operatorami i dostawcami technologii w celu zapobiegania efektom kaskadowym poprzez zastosowanie odpowiednich środków i usług,

— projektowanie i budowę sieci łączności i sterowania w celu ograniczenia skutków wszelkich błędów fizycznych i logicznych do ograniczonych części sieci oraz zapewnienia odpowiednich i szybkich środków łagodzących.

DOTYCHCZASOWA I NAJNOWOCZEŚNIEJSZA TECHNOLOGIA

9. Państwa członkowskie powinny zapewnić, aby odpowiednie zainteresowane strony, w szczególności operatorzy sieci energetycznych i dostawcy technologii, a zwłaszcza operatorzy usług kluczowych określeni na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji, wdrażały odpowiednie środki w zakresie gotowości związane z cyberbezpieczeństwem odnoszące się do połączenia dotychczasowej i najnowocześniejszej technologii w sektorze energetycznym. W dzisiejszym systemie energetycznym współistnieją dwa rodzaje technologii: starsza technologia o żywotności od 30 do 60 lat zaprojektowana, zanim uwzględniano kwestie cyberbezpieczeństwa oraz nowoczesne wyposażenie odzwierciedlające najnowocześniejszą cyfryzację i najnowocześniejsze urządzenia inteligentne.

10. Stosując niniejsze zalecenie, państwa członkowskie powinny zachęcać operatorów sieci energetycznych i dostawców technologii do stosowania, tam gdzie to możliwe, uznanych w skali międzynarodowej norm w zakresie cyberbezpieczeństwa. Jednocześnie zainteresowane strony i klienci, łącząc urządzenia z siecią, powinni stosować podejście zorientowane na cyberbezpieczeństwo.

11. W szczególności dostawcy technologii powinni zapewnić sprawdzone rozwiązania problemów związanych z bezpieczeństwem w dotychczasowych lub nowych technologiach bezpłatnie i bezzwłocznie po stwierdzeniu występowania istotnego problemu związanego z bezpieczeństwem.

12. W szczególności operatorzy sieci energetycznych powinni:

a) analizować zagrożenia związane z łączeniem koncepcji dotychczasowych z internetem rzeczy oraz mieć świadomość wewnętrznych i zewnętrznych interfejsów oraz ich podatności na zagrożenia;

b) podejmować odpowiednie środki przeciwko celowym atakom pochodzącym z dużej liczby celowo kontrolowanych urządzeń lub aplikacji konsumenckich;

c) ustanowić zdolność automatycznego monitorowania i analizowania zdarzeń związanych z bezpieczeństwem w środowiskach dotychczasowych technologii i internetu rzeczy, takich jak nieskuteczne próby zalogowania się, systemy alarmowe drzwi uruchamiane przy otwieraniu szafy lub inne zdarzenia;

d) regularnie przeprowadzać szczegółową analizę ryzyka w zakresie cyberbezpieczeństwa w odniesieniu do wszystkich dotychczasowych instalacji, zwłaszcza w przypadku łączenia starych i nowych technologii; ponieważ na dotychczasowe instalacje często składa się bardzo duża liczba aktywów, analizę ryzyka można przeprowadzić w podziale na klasy aktywów;

e) w stosownych przypadkach aktualizować oprogramowanie i sprzęt komputerowy w systemach dotychczasowych i internetu rzeczy do najnowszej wersji; wykonując takie działania, operatorzy powinni rozważyć środki uzupełniające, takie jak segregacja systemów lub dodanie zewnętrznych barier ochronnych, w przypadku gdy należałoby zainstalować poprawkę lub przeprowadzić aktualizację, ale nie jest to możliwe (np. w przypadku niewspieranych produktów);

f) formułować zamówienia, mając na uwadze cyberbezpieczeństwo, tj. żądać informacji na temat zabezpieczeń, żądać zgodności z istniejącymi normami w zakresie cyberbezpieczeństwa, zapewnić ciągłe ostrzeganie, poprawianie i przedstawianie propozycji łagodzenia skutków w przypadku wykrycia podatności na zagrożenia oraz wyjaśniać odpowiedzialność sprzedawcy w przypadku cyberataków lub incydentów;

g) współpracować z dostawcami technologii w celu zastąpienia dotychczasowych systemów za każdym razem, gdy jest to korzystne z punktu widzenia bezpieczeństwa, ale uwzględnić krytyczne funkcje systemu.

MONITOROWANIE

13. Państwa członkowskie powinny przekazać Komisji w terminie 12 miesięcy po przyjęciu niniejszego zalecenia, a następnie przekazywać co dwa lata szczegółowe informacje dotyczące stanu wdrożenia niniejszego zalecenia za pośrednictwem grupy współpracy ds. bezpieczeństwa sieci i informacji.

PRZEGLĄD

14. Na podstawie informacji przedłożonych przez państwa członkowskie Komisja dokona przeglądu wdrożenia niniejszego zalecenia i oceni, czy konieczne są dalsze środki w porozumieniu z państwami członkowskimi i odpowiednimi zainteresowanymi stronami.

ADRESACI

15. Niniejsze zalecenie skierowane jest do państw członkowskich.

Sporządzono w Brukseli dnia 3 kwietnia 2019 r.

W imieniu Komisji
Miguel ARIAS CAÑETE
Członek Komisji