KOMISJA
EUROPEJSKA

Bruksela, dnia 13.9.2017 r.
C(2017) 6100 final

ZALECENIE KOMISJI

z dnia 13.9.2017 r.

w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę

ZALECENIE KOMISJI

z dnia 13.9.2017 r.

w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę

KOMISJA EUROPEJSKA,

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

a także mając na uwadze, co następuje:

(1) Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich zyskały podstawowe znaczenie we wszystkich sektorach działalności gospodarczej, gdyż przedsiębiorstwa i obywatele są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej. Incydent cybernetyczny mający negatywne skutki dla organizacji w więcej niż jednym państwie członkowskim, a nawet dla całej Unii, i mogący spowodować poważne zakłócenia w funkcjonowaniu rynku wewnętrznego oraz – w szerszym wymiarze – w funkcjonowaniu sieci i systemów informatycznych mających zasadnicze znaczenie dla gospodarki, demokracji i społeczeństwa, to scenariusz, na który państwa członkowskie i instytucje UE muszą być dobrze przygotowane.

(2) Incydent cybernetyczny może zostać uznany za sytuację kryzysową na szczeblu Unii, jeżeli wywołane nim zakłócenia mają zbyt duży zakres, by państwo członkowskie, w którym doszło do tego incydentu, poradziło sobie z nim w pojedynkę, albo jeżeli dla dwóch lub większej liczby państw członkowskich ma on skutki o tak szerokim zakresie i o tak dużym znaczeniu technicznym lub politycznym, że wymaga on szybkiej koordynacji i reakcji na szczeblu politycznym Unii.

(3) Incydenty cybernetyczne mogą doprowadzić do kryzysu na szerszą skalę, odbijającego się negatywnie na sektorach działalności niezwiązanych z siecią i systemami informatycznymi ani z sieciami łączności; każda właściwa reakcja musi opierać się na ograniczających zagrożenie działaniach zarówno w domenie cyfrowej, jak i poza nią.

(4) Incydenty cybernetyczne są nieprzewidywalne, często pojawiają się i rozwijają w bardzo krótkim czasie, w związku z tym dotknięte ich skutkami podmioty i jednostki odpowiadające za reagowanie na incydenty i ograniczanie ich skutków muszą koordynować swoje działania w trybie pilnym. Ponadto incydenty cybernetyczne często nie są ograniczone do konkretnego obszaru geograficznego i mogą występować jednocześnie lub rozprzestrzeniać się błyskawicznie w wielu państwach.

(5) Skuteczne reagowanie na szczeblu UE na incydenty i kryzysy cybernetyczne na dużą skalę wymaga szybkiej i skutecznej współpracy między wszystkimi odpowiednimi zainteresowanymi stronami, a podstawowym warunkiem skutecznej reakcji jest gotowość i zdolności poszczególnych państw członkowskich do podejmowania określonych działań, a także skoordynowane wspólne działanie wspierane zdolnościami na szczeblu unijnym. Szybkie i skuteczne reagowanie na incydenty uzależnione jest więc od istnienia wcześniej ustanowionych i, w miarę możliwości,

dobrze przećwiczonych procedur i mechanizmów współpracy, w których kluczowe podmioty na szczeblu krajowym i unijnym mają jasno określone role i obowiązki.

(6) W konkluzjach[1] w sprawie ochrony krytycznej infrastruktury teleinformatycznej z dnia 27 maja 2011 r. Rada wezwała państwa członkowskie UE, aby wzmocniły wzajemną współpracę „i przyczyniły się, na podstawie doświadczeń i wyników krajowych w zakresie zarządzania kryzysowego oraz we współpracy z ENISA, do opracowania europejskich mechanizmów współpracy na wypadek incydentu cybernetycznego, które zostaną przetestowane w ramach następnego ćwiczenia *Cyber Europe* w 2012 roku".

(7) W komunikacie z 2016 r. „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego"[2] zachęcono państwa członkowskie do maksymalnego wykorzystania mechanizmów współpracy ustanowionych dyrektywą w sprawie bezpieczeństwa sieci i informacji[3] oraz do zacieśnienia współpracy transgranicznej związanej z gotowością na wypadek incydentu cybernetycznego na dużą skalę. Dodano w nim, że skoordynowane podejście do współpracy w sytuacjach kryzysowych pomiędzy różnymi elementami ekosystemu cybernetycznego, które należałoby określić w planie działania, zwiększyłoby stopień gotowości, a taki plan działania powinien również zapewniać synergię i spójność z istniejącymi mechanizmami zarządzania kryzysowego.

(8) W konkluzjach Rady[4] dotyczących wspomnianego wyżej komunikatu państwa członkowskie wezwały Komisję do przedłożenia takiego planu (projektu) współpracy do rozważenia przez podmioty działające na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji i inne zainteresowane strony. We wspomnianej dyrektywie nie określono jednak ram współpracy unijnej w przypadku incydentów i kryzysów cybernetycznych na dużą skalę.

(9) Komisja zasięgnęła opinii państw członkowskich w ramach dwóch odrębnych warsztatów konsultacyjnych, które odbyły się w dniach 5 kwietnia i 4 lipca 2017 r. w Brukseli z udziałem przedstawicieli zespołów reagowania na incydenty komputerowe (CSIRT) z państw członkowskich, grupy współpracy powołanej dyrektywą w sprawie bezpieczeństwa sieci i informacji oraz działającej w Radzie Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni, jak również przedstawicieli Europejskiej Służby Działań Zewnętrznych (ESDZ), ENISA, działu EC3 w Europolu i Sekretariatu Generalnego Rady (SGR).

(10) Obecny plan działania na rzecz skoordynowanego reagowania na szczeblu unijnym na incydenty i kryzysy cybernetyczne na dużą skalę, załączony do niniejszego zalecenia, jest rezultatem wspomnianych konsultacji i stanowi uzupełnienie komunikatu „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego".

---

1 Konkluzje Rady w sprawie ochrony krytycznej infrastruktury teleinformatycznej „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni", dokument 10299/11, Bruksela, 27 maja 2011 r.

2 COM(2016) 410 final z dnia 5 lipca 2016 r.

3 Dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii („dyrektywa w sprawie bezpieczeństwa sieci i informacji"), której celem jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

4 Dokument 14540/16 z dnia 15 listopada 2016 r.

(11) W planie tym określono i opisano cele i tryby współpracy między państwami członkowskimi UE a unijnymi instytucjami, organami, jednostkami organizacyjnymi i agencjami (zwanymi dalej „instytucjami unijnymi") przy reagowaniu na incydenty i kryzysy cybernetyczne na dużą skalę, a także sposoby pełnego wykorzystania w istniejących mechanizmach zarządzania kryzysowego istniejących podmiotów odpowiedzialnych za bezpieczeństwo cybernetyczne na szczeblu unijnym.

(12) W przypadku kryzysu cybernetycznego w rozumieniu motywu 2 koordynacja reakcji na szczeblu politycznym Unii w Radzie oparta zostanie na zintegrowanych uzgodnieniach UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych[5] (ang. *Integrated Political Crisis Response*, IPCR); Komisja będzie korzystać z mechanizmu ARGUS[6] służącego do koordynacji działań na wysokim szczeblu w przypadku kryzysów międzysektorowych. Jeżeli sytuacja kryzysowa wiąże się z istotnymi kwestiami z zakresu polityki zewnętrznej lub wspólnej polityki bezpieczeństwa i obrony (WPBiO), uruchomiony zostanie mechanizm reagowania kryzysowego (ang. *Crisis Response Mechanism*, CRM)[7] Europejskiej Służby Działań Zewnętrznych (ESDZ).

(13) W pewnych obszarach w sektorowych mechanizmach zarządzania kryzysowego na szczeblu UE przewidziano współpracę w przypadku incydentów lub kryzysów cybernetycznych. Na przykład w ramach Europejskiego Globalnego Systemu Nawigacji Satelitarnej (GNSS) w decyzji Rady 2014/496/WPZiB z dnia 22 lipca 2014 r. w sprawie aspektów wdrażania, działania i użytkowania europejskiego globalnego systemu nawigacji satelitarnej mających wpływ na bezpieczeństwo Unii Europejskiej określono już role przydzielone Radzie, Wysokiemu Przedstawicielowi, Komisji, Agencji Europejskiego GNSS i państwom członkowskim w łańcuchu odpowiedzialności operacyjnej ustanowionym na potrzeby reagowania na zagrożenia dla Unii, państw członkowskich lub GNSS, w tym zagrożenie stwarzane przez ataki cybernetyczne. W związku z tym niniejsze zalecenie nie powinno naruszać funkcjonowania takich mechanizmów.

(14) Odpowiedzialność za reagowanie na incydenty lub kryzysy cybernetyczne na dużą skalę spoczywa w pierwszej kolejności na państwach członkowskich nimi dotkniętych. Komisja, Wysoki Przedstawiciel i inne instytucje lub służby unijne odgrywają jednak ważną rolę, wynikającą z prawa Unii lub z faktu, że incydenty i kryzysy cybernetyczne mogą mieć negatywne skutki dla wszystkich sektorów działalności gospodarczej w ramach jednolitego rynku, dla bezpieczeństwa i stosunków międzynarodowych Unii, a także dla samych instytucji.

(15) Na szczeblu UE do głównych podmiotów zaangażowanych w reagowanie na kryzysy cybernetyczne należą nowe struktury i mechanizmy ustanowione na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji, a mianowicie sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz stosowne agencje i jednostki organizacyjne, tj. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europejskie Centrum ds. Walki z Cyberprzestępczością w Europolu (Europol/EC3), Centrum Analiz Wywiadowczych UE (INTCEN), Dyrekcja ds. Wywiadu w Sztabie Wojskowym UE (EUMS INT) oraz Centrum

---

5 Więcej informacji na ten temat podano w sekcji 3.1 dodatku dotyczącego zarządzania kryzysowego, mechanizmów współpracy i podmiotów na szczeblu UE.

6 *Ibidem*.

7 *Ibidem*.

Sytuacyjne (SITROOM), działające wspólnie jako SIAC (pojedyncza komórka analiz wywiadowczych), a ponadto komórka UE ds. syntezy informacji o zagrożeniach hybrydowych (działająca przy INTCEN), zespół reagowania na incydenty komputerowe w instytucjach i agencjach UE (CERT-UE) oraz Centrum Koordynacji Reagowania Kryzysowego działające w Komisji Europejskiej.

(16) Współpraca państw członkowskich w zakresie reagowania na incydenty cybernetyczne na poziomie technicznym prowadzona jest za pośrednictwem sieci CSIRT ustanowionej dyrektywą w sprawie bezpieczeństwa sieci i informacji. ENISA zapewnia tej sieci obsługę sekretariatu i aktywnie wspiera współpracę między poszczególnymi zespołami CSIRT. Krajowe CSIRT oraz CERT-UE podejmują współpracę i wymieniają się informacjami na zasadzie dobrowolności, w tym, w razie potrzeby, przy reagowaniu na incydenty cybernetyczne mające negatywne skutki dla jednego państwa członkowskiego lub większej ich liczby. Na wniosek przedstawiciela CSIRT jednego z państw członkowskich mogą one omówić oraz, w miarę możliwości, ustalić sposób skoordynowanej reakcji na incydent, który wykryto na obszarze jurysdykcji tego państwa członkowskiego. Odnośne procedury zostaną określone w standardowych procedurach operacyjnych (SOP)[8] sieci CSIRT.

(17) Do zadań sieci CSIRT należy również omawianie, analizowanie i określanie dalszych form współpracy operacyjnej, w tym kwestii związanych z kategoriami zagrożeń i incydentów, wczesnym ostrzeganiem, wzajemną pomocą oraz zasadami i trybami koordynacji, w przypadku gdy państwa członkowskie podejmują działania w reakcji na transgraniczne zagrożenia i incydenty.

(18) Zadaniem grupy współpracy, powołanej na mocy art. 11 dyrektywy w sprawie bezpieczeństwa sieci i informacji, jest udzielanie strategicznych wskazówek dotyczących działalności sieci CSIRT oraz omawianie zdolności i gotowości państw członkowskich, a także, na zasadzie dobrowolności, ocena krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych oraz skuteczności CSIRT oraz wskazywanie najlepszych praktyk.

(19) Osobnym obszarem prac prowadzonych przez grupę współpracy są wytyczne w zakresie zgłaszania incydentów, zgodnie z art. 14 ust. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji, dotyczące okoliczności, w których operatorzy usług kluczowych są zobowiązani do zgłaszania incydentów zgodnie z art. 14 ust. 3, oraz formatu i procedury takich zgłoszeń[9].

(20) Orientowanie się w czasie rzeczywistym w sytuacji, podejmowanym ryzyku i w zagrożeniach oraz ich zrozumienie, uzyskane dzięki zgłoszeniom, ocenom, badaniom, dochodzeniom i analizom, jest niezbędne do podejmowania świadomych decyzji. Taka orientacja sytuacyjna – u wszystkich zainteresowanych stron – ma kluczowe znaczenie w zapewnianiu skutecznej i skoordynowanej reakcji. Orientacja sytuacyjna obejmuje informacje zarówno o przyczynach, jak i skutkach oraz źródle incydentu. Powszechnie przyjmuje się, że taką orientację można osiągnąć tylko w drodze wymiany i udostępniania przez zainteresowane strony informacji w odpowiednim formacie, przy użyciu wspólnej taksonomii do opisu incydentu oraz w sposób zapewniający odpowiedni poziom bezpieczeństwa.

---

8 W opracowaniu; oczekuje się, że zostaną przyjęte do końca 2017 r.

9 Wytyczne te mają zostać opracowane do końca 2017 r.

(21) Reagowanie na incydenty cybernetyczne może przybierać różne formy, począwszy od określenia środków technicznych, mogących polegać na wspólnej analizie technicznych przyczyn incydentu (np. analizie złośliwego oprogramowania) przez dwa podmioty lub większą ich liczbę, lub określenia sposobów, za pomocą których organizacje mogą sprawdzić, czy padły ofiarami incydentu (np. oznaki naruszenia integralności systemu), po decyzje operacyjne dotyczące stosowania takich środków oraz – na szczeblu politycznym – decyzje o wykorzystaniu innych instrumentów, takich jak ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne[10] lub unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym[11], w zależności od charakteru incydentu.

(22) Zaufanie europejskich obywateli i przedsiębiorstw do usług cyfrowych ma kluczowe znaczenie dla dynamicznie rozwijającego się jednolitego rynku cyfrowego. W związku z tym komunikacja podczas sytuacji kryzysowej odgrywa szczególnie ważną rolę w ograniczaniu negatywnych skutków incydentów i kryzysów cybernetycznych. Komunikację można również wykorzystać w ramach wspólnej reakcji dyplomatycznej jako środek wpływania na zachowania (potencjalnych) sprawców działających z terytorium państw trzecich. Uspójnienie informacji publikowanych w celu ograniczenia negatywnych skutków incydentów i kryzysów cybernetycznych z informacjami publikowanymi w celu wywierania wpływu na sprawców ma zasadnicze znaczenie dla zapewnienia skuteczności reakcji politycznej.

(23) Informowanie obywateli o tym, w jaki sposób mogą ograniczyć negatywne skutki danego incydentu na poziomie indywidualnego użytkownika bądź organizacji (na przykład poprzez aktualizację oprogramowania lub podjęcie działań uzupełniających w celu uniknięcia zagrożenia) może być skutecznym środkiem ograniczania szkodliwości incydentu lub kryzysu cybernetycznego na dużą skalę.

(24) Komisja, korzystając z infrastruktury usług cyfrowych w zakresie bezpieczeństwa cybernetycznego w ramach instrumentu „Łącząc Europę”, tworzy mechanizm w postaci platformy usług podstawowych, którą nazwano MeliCERTes, służący współpracy między CSIRT uczestniczących państw członkowskich, w celu poprawy poziomu ich gotowości, udoskonalenia ich współdziałania i reakcji na pojawiające się zagrożenia i incydenty cybernetyczne. Komisja, w drodze konkurencyjnych zaproszeń do składania wniosków o przyznanie dotacji ze środków instrumentu „Łącząc Europę”, współfinansuje CSIRT w państwach członkowskich, aby zwiększyć ich zdolności operacyjne na szczeblu krajowym.

(25) Ćwiczenia w dziedzinie bezpieczeństwa cybernetycznego na szczeblu UE są niezbędne do stymulowania i poprawy współpracy między państwami członkowskimi a sektorem prywatnym. W tym celu od 2010 r. ENISA organizuje regularnie ćwiczenia w zakresie incydentów cybernetycznych na skalę ogólnoeuropejską („Cyber Europe”).

(26) W konkluzjach Rady[12] w sprawie realizacji wspólnej deklaracji przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i Sekretarza Generalnego Organizacji Traktatu Północnoatlantyckiego zaapelowano o wzmocnienie współpracy

---

10 Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej”), dokument 9916/17.

11 Wspólny dokument roboczy służb „Unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym” („Unijny podręcznik taktyczny”), SWD(2016) 227 final z 5.7.2016.

12 Dokument 15283/16 z dnia 6 grudnia 2016 r.

w zakresie ćwiczeń w dziedzinie bezpieczeństwa cybernetycznego poprzez wzajemny udział pracowników w odpowiednich ćwiczeniach, w tym w szczególności ćwiczeniach „Cyber Coalition” oraz „Cyber Europe”.

(27) Stale zmieniający się obraz zagrożeń i niedawne incydenty cybernetyczne są oznaką rosnącego ryzyka, na jakie narażona jest Unia, państwa członkowskie powinny zatem bez dalszych opóźnień, a w każdym razie przed końcem 2018 r., podjąć działania w oparciu o niniejsze zalecenie,

PRZYJMUJE NINIEJSZE ZALECENIE:

1. Państwa członkowskie i instytucje unijne powinny ustanowić unijne ramy reagowania w sytuacji kryzysu cybernetycznego, obejmujące cele i tryby współpracy przedstawione w planie działania, z uwzględnieniem określonych w nim zasad przewodnich.

2. W unijnych ramach reagowania w sytuacji kryzysu cybernetycznego należy w szczególności określić właściwe podmioty, instytucje unijne i organy państw członkowskich, na wszystkich niezbędnych poziomach – technicznym, operacyjnym, strategicznym/politycznym – oraz opracować, w stosownych przypadkach, standardowe procedury operacyjne zawierające opis trybu współpracy tych podmiotów w ramach unijnych mechanizmów zarządzania kryzysowego. Należy położyć nacisk na umożliwienie wymiany informacji bez zbędnej zwłoki i koordynowanie reakcji w obliczu incydentów i kryzysów cybernetycznych na dużą skalę.

3. W tym celu właściwe organy państw członkowskich powinny wspólnie wypracować dalsze szczegóły protokołów wymiany informacji i współpracy. Grupa współpracy powinna dzielić się doświadczeniami w tych kwestiach z odpowiednimi instytucjami unijnymi.

4. Państwa członkowskie powinny zapewnić, by ich krajowe mechanizmy zarządzania kryzysowego umożliwiały adekwatną reakcję na incydent cybernetyczny, jak również by określono w nich procedury konieczne do umożliwienia współpracy na szczeblu UE w oparciu o ramy unijne.

5. W odniesieniu do istniejących unijnych mechanizmów zarządzania kryzysowego, zgodnie z planem działania, państwa członkowskie, wraz ze służbami Komisji i ESDZ, powinny określić praktyczne wytyczne wdrożeniowe, dotyczące zintegrowania krajowych podmiotów i procedur zarządzania kryzysowego i bezpieczeństwa cybernetycznego z istniejącymi unijnymi mechanizmami zarządzania kryzysowego, a mianowicie IPCR i mechanizmem reagowania kryzysowego ESDZ. Państwa członkowskie powinny w szczególności zapewnić utworzenie odpowiednich struktur umożliwiających skuteczny przepływ informacji między swoimi krajowymi organami zarządzania kryzysowego a swoimi przedstawicielami na szczeblu UE, zaangażowanymi w funkcjonowanie unijnych mechanizmów kryzysowych.

6. Państwa członkowskie powinny w pełni wykorzystywać możliwości, jakie oferuje program infrastruktury usług cyfrowych (DSI) w zakresie bezpieczeństwa cybernetycznego w ramach instrumentu „Łącząc Europę”, a także współpracować z Komisją w celu zapewnienia, by mechanizm współpracy w postaci platformy usług podstawowych, obecnie w opracowaniu, zapewniał niezbędne funkcje i spełniał wymogi w zakresie współpracy, również podczas kryzysów cybernetycznych.

7. Państwa członkowskie – przy wsparciu ENISA, a także w oparciu o wcześniejsze prace w tej dziedzinie – powinny współpracować przy opracowywaniu i przyjmowaniu wspólnej taksonomii i wzoru raportów sytuacyjnych na potrzeby opisu technicznych przyczyn i skutków incydentów cybernetycznych, aby dalej zacieśniać swoją współpracę techniczną i operacyjną w sytuacjach kryzysowych. Państwa członkowskie powinny zatem uwzględnić prowadzone przez grupę współpracy bieżące prace nad wytycznymi w zakresie zgłaszania incydentów, a w szczególności aspekty dotyczące formatów zgłoszeń krajowych.

8. Procedury określone we wspomnianych ramach powinny być testowane i w razie konieczności zmieniane w następstwie nowych doświadczeń zdobywanych przez państwa członkowskie w wyniku ich uczestnictwa w krajowych, regionalnych i unijnych inicjatywach, jak również ćwiczeniach z zakresu dyplomacji cyfrowej oraz ćwiczeniach NATO w dziedzinie bezpieczeństwa cybernetycznego. W szczególności procedury te powinny być przedmiotem testów w kontekście ćwiczeń „Cyber Europe” organizowanych przez ENISA. Ćwiczenia „Cyber Europe” 2018 będą stanowić pierwszą tego rodzaju okazję.

9. Państwa członkowskie i instytucje unijne powinny regularnie ćwiczyć w skali krajowej i ogólnoeuropejskiej swoją reakcję na incydenty i kryzysy cybernetyczne na dużą skalę, w tym, w razie potrzeby, swoją odpowiedź polityczną, również przy zaangażowaniu, w stosownych przypadkach, podmiotów z sektora prywatnego.

Sporządzono w Brukseli dnia 13.9.2017 r.

W imieniu Komisji
Mariya GABRIEL
Członek Komisji

ODPIS UWIERZYTELNIONY
W imieniu Sekretarza Generalnego

Jordi AYET PUIGARNAU
Dyrektor Kancelarii
KOMISJA EUROPEJSKA