KOMISJA
EUROPEJSKA

Bruksela, dnia 7.2.2013
SWD(2013) 31 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

Towarzyszący dokumentowi

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady

w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

{COM(2013) 48 final}
{SWD(2013) 32 final}

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

Towarzyszący dokumentowi

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady

w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

1. ZAKRES

Niniejsza ocena skutków dotyczy wariantów strategicznych mających na celu poprawę bezpieczeństwa internetu oraz innych sieci i systemów informatycznych wykorzystywanych na potrzeby świadczenia usług istotnych dla funkcjonowania naszego społeczeństwa (takich jak np. administracja publiczna, usługi finansowe i bankowe, usługi energetyczne, transportowe i w zakresie ochrony zdrowia, a także określone usługi internetowe umożliwiające istotne procesy gospodarcze i społeczne, np. platformy handlu elektronicznego i serwisy społecznościowe). Ten obszar zagadnień określany jest mianem bezpieczeństwa sieci i informacji (NIS, z ang. *network and information security*).

2. KONTEKST POLITYCZNY

Na rosnące znaczenie kwestii bezpieczeństwa sieci i informacji dla naszych gospodarek i społeczeństw Komisja po raz pierwszy zwróciła uwagę w 2001 r. Aby zapewnić wysoki i skuteczny poziom bezpieczeństwa sieci i informacji w UE, w 2004 r. Unia Europejska postanowiła utworzyć Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA). Stosowane dotychczas przez UE podejście do kwestii bezpieczeństwa sieci i informacji polegało głównie na przyjęciu szeregu planów działania oraz strategii, w których państwa członkowskie wezwano do zwiększenia zdolności w zakresie zapewniania bezpieczeństwa sieci i informacji oraz do współpracy przy rozwiązywaniu transgranicznych problemów w tym obszarze.

Z zainteresowanymi stronami przeprowadzono konsultacje poświęcone różnym aspektom inicjatywy (takim jak określenie problemu oraz możliwe sposoby zlikwidowania istniejących niedociągnięć), które odbyły się w drodze:

- **internetowych konsultacji społecznych** dotyczących „poprawy bezpieczeństwa sieci i informacji w UE", które trwały od 23 lipca do 15 października 2012 r.; za pośrednictwem narzędzia internetowego otrzymano łącznie 169 odpowiedzi, a kolejnych 10 zostało przesłanych Komisji w formie pisemnej;
- rozmów z przedstawicielami **państw członkowskich** w ramach europejskiego forum państw członkowskich (EFMS), w trakcie spotkań dwustronnych oraz na unijnej konferencji poświęconej bezpieczeństwu cybernetycznemu, którą Komisja i Europejska Służba Działań Zewnętrznych zorganizowały w dniu 6 lipca 2012 r.;
- rozmów z przedstawicielami przedsiębiorstw i stowarzyszeń z **sektora prywatnego** prowadzonych w ramach europejskiego partnerstwa publiczno-prywatnego na rzecz odporności kluczowej infrastruktury informacyjnej (EP3R) oraz w trakcie spotkań dwustronnych;
- rozmów z **ENISA i CERT-UE**;

- rozmów prowadzonych na forum **zgromadzenia agendy cyfrowej w 2012 r.**

3. OPIS PROBLEMU

3.1. Definicja problemu

Problem można opisać jako ogólnie ***niewystarczający poziom ochrony przed incydentami i zagrożeniami w obszarze bezpieczeństwa sieci i informacji w obrębie całej UE, które mają negatywny wpływ na właściwe funkcjonowanie rynku wewnętrznego***.

W obliczu faktu, że sieci i systemy informatyczne są wzajemnie powiązane, a internet ma charakter globalny, zasięg wielu incydentów w zakresie bezpieczeństwa sieci i informacji wykracza poza granice krajowe i zagraża funkcjonowaniu rynku wewnętrznego.

Dostęp do usług transgranicznych może zostać zawieszony lub przerwany w wyniku naruszenia bezpieczeństwa, jak to miało miejsce w przypadku ataków na eBay i PayPal. Konieczność szybkiego reagowania celem rozwiązania problemów oraz potrzebę wymiany informacji na temat poważnych incydentów uwidocznił przypadek ataków na Diginotar, niderlandzką spółkę zajmującą się wystawianiem certyfikatów internetowych. W następstwie tego rodzaju incydentów państwa członkowskie rozpoczęły wprowadzanie własnych regulacji. Nieskoordynowane interwencje regulacyjne mogą prowadzić do fragmentacji i powstania barier na rynku wewnętrznym, które będą oznaczały wyższe koszty przestrzegania przepisów dla przedsiębiorstw działających w więcej niż jednym państwie członkowskim.

Problem ten dotyczy całego społeczeństwa i całej gospodarki (zarówno organów administracji publicznej, jak i przedsiębiorstw oraz konsumentów). W szczególności szereg branż odgrywa zasadniczą rolę w świadczeniu kluczowych usług wspierających funkcjonowanie naszych gospodarek i społeczeństw, a bezpieczeństwo ich systemów ma szczególne znaczenie dla funkcjonowania rynku wewnętrznego. Branże te obejmują banki, giełdy papierów wartościowych, produkcję, przesył i dystrybucję energii, transport (lotniczy, kolejowy, morski), ochronę zdrowia, infrastrukturę podstawowych usług internetowych oraz administrację publiczną. Konsultacje społeczne pokazały silne poparcie zainteresowanych stron dla zajęcia się kwestią bezpieczeństwa sieci i informacji w tych branżach oraz podjęcia odpowiednich działań na poziomie UE.

Jeżeli nie zostaną zastosowane żadne dodatkowe środki w celu przeciwdziałania rosnącej liczbie incydentów, ucierpieć może na tym zaufanie konsumentów do usług internetowych, co z kolei może mieć negatywny wpływ na osiągnięcie celów wyznaczonych w agendzie cyfrowej.

3.2. Czynniki mające wpływ na problem

Na stwierdzony problem wpływa szereg czynników.

Po pierwsze, **w obrębie UE stwierdzić można niejednolity poziom zdolności na poziomie krajowym**, co utrudnia osiągnięcie atmosfery wzajemnego zaufania, które jest warunkiem wstępnym współpracy i wymiany informacji.

Po drugie, **wymiana informacji na temat incydentów i zagrożeń jest niedostateczna**. Większość incydentów w zakresie bezpieczeństwa sieci i informacji jest niezgłaszana i pozostaje niezauważona, głównie w wyniku niechęci przedsiębiorstw do ujawnienia odpowiednich informacji ze względu na obawy związane z możliwą szkodą dla reputacji lub roszczeniami z tytułu odpowiedzialności. Wymiana informacji w ramach istniejących partnerstw i platform publiczno-prywatnych, takich jak EFMS i EP3R, ogranicza się do najlepszych praktyk.

4. EFEKTYWNOŚĆ ISTNIEJĄCYCH ŚRODKÓW

4.1. Luki w istniejących ramach regulacyjnych

Obowiązujące przepisy nakładają jedynie na przedsiębiorstwa telekomunikacyjne wymóg przyjęcia środków przeciwdziałania zagrożeniom związanym z bezpieczeństwem sieci i informacji oraz zgłaszania incydentów w tym zakresie, mimo iż wszystkie podmioty uzależnione od sieci i systemów informatycznych stoją w obliczu zagrożeń związanych z bezpieczeństwem. Prowadzi to do nierównych warunków prowadzenia działalności, gdyż ten sam incydent, dotykający np. klasycznego operatora telekomunikacyjnego oraz przedsiębiorstwo świadczące usługi telefonii internetowej, musiałby zostać zgłoszony właściwemu organowi krajowemu tylko w pierwszym przypadku.

Wszystkie podmioty będące administratorami danych (np. banki lub szpitale) są wprawdzie na mocy ram regulacyjnych w zakresie ochrony danych zobowiązane do ustanowienia środków bezpieczeństwa proporcjonalnych do istniejących zagrożeń, ale muszą zgłaszać jedynie naruszenia bezpieczeństwa prowadzące do naruszenia ochrony danych osobowych.

Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej obejmuje jedynie branże energetyki i transportu, przy czym dotychczas państwa członkowskie wskazały jedynie nieliczne tego rodzaju obiekty. Dyrektywa nie nakłada na operatorów obowiązku zgłaszania istotnych naruszeń bezpieczeństwa i nie ustanawia mechanizmów współpracy między państwami członkowskimi ani mechanizmów reagowania na incydenty.

Współprawodawcy europejscy omawiają obecnie wniosek Komisji w sprawie dyrektywy dotyczącej ataków na systemy informatyczne[1]. Wniosek ten służy wyłącznie kryminalizacji określonych rodzajów postępowania, ale nie dotyczy kwestii zapobiegania zagrożeniom i incydentom związanym z bezpieczeństwem sieci i informacji, reagowania na incydenty w tym zakresie oraz ograniczania ich skutków.

4.2. Granice podejścia opartego na dobrowolności

Stosowane dotychczas podejście oparte na dobrowolności doprowadziło do niejednolitego poziomu gotowości i ograniczonego poziomu współpracy.

Zakres zadań EFMS jest ograniczony, gdyż państwa członkowskie nie prowadzą ani wymiany informacji na temat incydentów i zagrożeń, ani współpracy celem zwalczania zagrożeń o charakterze transgranicznym. EFMS nie ma uprawnień do zobowiązania swoich członków do zapewnienia określonych minimalnych zdolności.

ENISA nie posiada uprawnień operacyjnych i przykładowo nie może interweniować w celu rozwiązania problemów w zakresie bezpieczeństwa sieci i informacji.

EP3R nie ma żadnych formalnych uprawnień, w związku z czym nie może żądać od podmiotów sektora prywatnego zgłaszania incydentów organom krajowym. W obrębie EP3R nie istnieją również ramy umożliwiające wymianę informacji poufnych lub przekazywanie informacji na temat zagrożeń i incydentów związanych z bezpieczeństwem sieci i informacji.

5. KONIECZNOŚĆ PODJĘCIA DZIAŁAŃ NA POZIOMIE UE, KWESTIE POMOCNICZOŚCI I PROPORCJONALNOŚCI

Zagwarantowanie bezpieczeństwa sieci i informacji ma zasadnicze znaczenie dla właściwego funkcjonowania rynku wewnętrznego i dobrobytu społecznego. Właściwą podstawę prawną

[1] COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:PL:PDF

zharmonizowania wymogów w zakresie bezpieczeństwa sieci i informacji oraz wprowadzenia minimalnego wspólnego poziomu bezpieczeństwa w całej UE stanowi artykuł 114 Traktatu o funkcjonowaniu Unii Europejskiej.

Podjęcie przez Unię działań w obszarze bezpieczeństwa sieci i informacji jest uzasadnione z punktu widzenia zasady **pomocniczości** ze względu na transgraniczny charakter problemu oraz większą efektywność (a tym samym wartość dodaną) działań na poziomie UE w porównaniu z istniejącymi strategiami krajowymi.

Aby zapewnić współpracę między wszystkimi państwami członkowskimi konieczne jest zagwarantowanie, że wszystkie z nich dysponują wymaganym minimalnym poziomem zdolności. Ponadto oczywiste jest, że uzgodnione i oparte na współpracy działania polityczne w zakresie bezpieczeństwa sieci i informacji mogą mieć istotny korzystny wpływ na skuteczną ochronę praw podstawowych, a zwłaszcza prawa do ochrony danych osobowych i prywatności.

Środki składające się na preferowany wariant są uzasadnione z punktu widzenia zasady **proporcjonalności**, zważywszy że wymogi dla państw członkowskich zostały ustanowione na poziomie minimalnym niezbędnym do osiągnięcia właściwej gotowości oraz do umożliwienia współpracy opartej na wzajemnym zaufaniu, a nałożone na przedsiębiorstwa i organy administracji publicznej wymogi dotyczące przeciwdziałania zagrożeniom oraz zgłaszania incydentów obejmują wyłącznie podmioty o znaczeniu krytycznym i nakładają środki, które są proporcjonalne do zagrożeń i dotyczą incydentów o znacznych skutkach. Środki składające się na preferowany wariant nie prowadzą również do nieproporcjonalnych kosztów.

6. CELE

Celem nadrzędnym jest zwiększenie w całej UE poziomu ochrony przed incydentami i zagrożeniami w zakresie bezpieczeństwa sieci i informacji. Cele szczegółowe są następujące:

- **cel nr 1** – ustanowienie minimalnego wspólnego poziomu bezpieczeństwa sieci i informacji w państwach członkowskich, a tym samym zwiększenie ogólnego poziomu gotowości i możliwości reagowania;
- **cel nr 2** – poprawa współpracy w zakresie bezpieczeństwa sieci i informacji na poziomie UE w celu efektywnego zwalczania incydentów i zagrożeń o charakterze transgranicznym;
- **cel nr 3** – rozwój kultury przeciwdziałania zagrożeniom i poprawa wymiany informacji między sektorem publicznym i prywatnym.

7. WARIANTY STRATEGICZNE

Warianty strategiczne uwzględnione w ocenie skutków obejmują scenariusz kontynuacji dotychczasowych działań, podejście oparte na regulacji oraz podejście mieszane. Ewentualny wariant polegający na rezygnacji z wszelkich działań UE w obszarze bezpieczeństwa sieci i informacji odrzucono.

7.1. Wariant nr 1 – kontynuacja dotychczasowych działań (scenariusz odniesienia)

Komisja z pomocą ENISA miałaby kontynuować stosowanie aktualnego podejścia opartego na dobrowolności, zwracając się do państw członkowskich o budowę zdolności w zakresie bezpieczeństwa sieci i informacji na poziomie krajowym (np. zespoły reagowania na incydenty komputerowe, krajowe plany awaryjne na wypadek incydentów cybernetycznych, krajowe strategie bezpieczeństwa cybernetycznego) oraz o współpracę na poziomie UE (np.

przez sieć zespołów reagowania na incydenty komputerowe obejmującą całą Europę oraz europejski plan awaryjny na wypadek incydentów cybernetycznych i europejski plan współpracy).

7.2. Wariant nr 2 – podejście oparte na regulacji

Komisja zobowiązałaby wszystkie państwa członkowskie do stworzenia przynajmniej minimalnych zdolności krajowych (zespoły reagowania na incydenty komputerowe, właściwe organy, krajowe plany awaryjne na wypadek incydentów cybernetycznych, krajowe strategie bezpieczeństwa cybernetycznego).

W ramach tego wariantu właściwe organy krajowe oraz zespoły reagowania na incydenty komputerowe stanowiłyby elementy **sieci** służącej współpracy na poziomie UE. W obrębie tej sieci organy krajowe i zespoły reagowania na incydenty komputerowe prowadziłyby wymianę informacji oraz współpracę w celu zwalczania zagrożeń i incydentów w obszarze bezpieczeństwa sieci i informacji zgodnie z **europejskim planem awaryjnym na wypadek incydentów cybernetycznych i europejskim planem współpracy**, które musiałyby zostać uzgodnione przez państwa członkowskie.

Przedsiębiorstwa (z wyjątkiem mikroprzedsiębiorstw) w określonych branżach o znaczeniu krytycznym, takich jak bankowość, energetyka (energia elektryczna i gaz ziemny), transport, ochrona zdrowia oraz infrastruktura podstawowych usług internetowych, jak również organy administracji publicznej zostałyby zobowiązane do oceny zagrożeń, przed którymi stoją, oraz przyjęcia właściwych i proporcjonalnych środków w odpowiedzi na faktyczne zagrożenia. Podmioty te zostałyby ponadto zobowiązane do zgłaszania właściwym organom incydentów, które mają znaczny negatywny wpływ na funkcjonowanie ich sieci i systemów informatycznych, a tym samym niosą ze sobą istotne skutki dla ciągłości świadczenia usług i prowadzenia dostaw towarów, które są uzależnione od tych sieci i systemów. Koncepcja ta odpowiada podejściu określonemu w art. 13a i 13b dyrektywy ramowej dotyczącej usług łączności elektronicznej.

7.3. Wariant nr 3 – podejście mieszane

Komisja dokonałaby połączenia dobrowolnych inicjatyw opartych na chęci państw członkowskich do współpracy, mających na celu ustanowienie lub wzmocnienie zdolności państw członkowskich w zakresie bezpieczeństwa sieci i informacji oraz ustanowienie mechanizmów współpracy na poziomie UE, z wymogami regulacyjnymi nałożonymi na kluczowe podmioty prywatne i organy administracji publicznej.

Dobrowolne inicjatywy byłyby zasadniczo podobne do tych, które uwzględniono w wariancie nr 1, natomiast wymogi regulacyjne byłyby identyczne z tymi, które zostały przewidziane w wariancie nr 2, zarówno jeśli chodzi o podmioty, których miałyby one dotyczyć, jak i treść nałożonych obowiązków.

ENISA zapewniłaby wsparcie i wiedzę specjalistyczną Komisji, państwom członkowskim i podmiotom sektora prywatnego, np. publikując wytyczne techniczne i zalecenia.

8. ANALIZA SKUTKÓW

Ocena obejmuje, oprócz kwestii poziomu bezpieczeństwa, skutki gospodarcze i społeczne każdego z trzech wariantów. Obejmuje ona również koszty, z którymi wiązałaby się realizacja wariantów nr 2 i 3.

Żaden z rozpatrywanych wariantów nie pociąga za sobą skutków dla środowiska, które można byłoby precyzyjnie przewidzieć.

8.1. Wariant nr 1 – kontynuacja dotychczasowych działań (scenariusz odniesienia)

Poziom bezpieczeństwa: Nieprawdopodobne jest, by wszystkie państwa członkowskie osiągnęły porównywalny krajowy poziom zdolności i gotowości niezbędnych do poprawy bezpieczeństwa oraz umożliwienia współpracy i wymiany informacji poufnych na poziomie UE. Niemożliwe byłoby osiągnięcie równych warunków w zakresie przeciwdziałania zagrożeniom i zwiększenia przejrzystości jeśli chodzi o incydenty; w dalszym ciągu istniałyby luki w ramach regulacyjnych.

Skutki gospodarcze: Skutki byłyby uzależnione od stopnia, w jakim państwa członkowskie stosowałyby się do zaleceń Komisji. Niedostateczny poziom bezpieczeństwa w mniej rozwiniętych państwach członkowskich prowadziłby do pogorszenia ich konkurencyjności oraz perspektyw wzrostu gospodarczego, narażając je na zagrożenia i incydenty. Biorąc pod uwagę aktualne trendy, incydenty w zakresie bezpieczeństwa sieci i informacji stawałyby się coraz bardziej widoczne dla przedsiębiorstw i konsumentów, tworząc przeszkodę dla zakończenia budowy rynku wewnętrznego.

Skutki społeczne: Utrzymywanie się, a prawdopodobnie nawet nasilenie incydentów i zagrożeń miałoby negatywny wpływ na zaufanie obywateli do środowiska internetowego.

8.2. Wariant nr 2 – podejście oparte na regulacji

Poziom bezpieczeństwa: Nałożone na państwa członkowskie zobowiązania zapewniłyby odpowiednią gotowość każdego z nich i przyczyniłyby się do stworzenia klimatu wzajemnego zaufania, który stanowi wstępny warunek skutecznej współpracy na poziomie UE.

Nałożenie na organy administracji publicznej i kluczowe podmioty sektora prywatnego wymogu przeciwdziałania zagrożeniom w zakresie bezpieczeństwa sieci i informacji tworzyłoby silną zachętę do właściwego szacowania zagrożeń dla bezpieczeństwa i efektywnego przeciwdziałania tym zagrożeniom. Łączne dodatkowe koszty, które musiałyby ponieść wszystkie stosowne branże w UE celem spełnienia tych wymogów, wahałyby się od **1 do 2 mld EUR**. Koszty przestrzegania przepisów przypadające **na jedno małe lub średnie przedsiębiorstwo** wahałyby się między **2500 a 5000 EUR**.

Skutki gospodarcze: W wyniku wyższego poziomu bezpieczeństwa doszłoby do ograniczenia strat finansowych spowodowanych incydentami i zagrożeniami w obszarze bezpieczeństwa sieci i informacji. Zaufanie przedsiębiorstw i konsumentów do środowiska cyfrowego zostałoby wzmocnione, co przyniosłoby korzyści rynkowi wewnętrznemu. Promowanie rozwiniętej kultury przeciwdziałania zagrożeniom pobudziłoby również popyt na bezpieczne produkty i rozwiązania w obszarze technologii informacyjno-telekomunikacyjnych.

Skutki społeczne: Wyższy poziom bezpieczeństwa prowadziłby do zwiększenia zaufania obywateli do środowiska internetowego, dzięki czemu mogliby oni czerpać pełnię korzyści z nim związanych (np. w postaci mediów społecznościowych, usług e-edukacji czy e-zdrowia).

8.3. Wariant nr 3 – podejście mieszane

Poziom bezpieczeństwa: Podobnie jak w przypadku wariantu nr 1, nie ma gwarancji, że poziom bezpieczeństwa wynikający z krajowych zdolności w zakresie bezpieczeństwa sieci i informacji oraz współpracy na poziomie UE uległby poprawie w wyniku dobrowolnych inicjatyw. Z drugiej zaś strony nałożenie na organy administracji publicznej i kluczowe podmioty sektora prywatnego wymogów w zakresie bezpieczeństwa sieci i informacji stworzyłoby silną zachętę do właściwego szacowania zagrożeń dla bezpieczeństwa i efektywnego przeciwdziałania tym zagrożeniom. Mechanizmy te byłyby jednak nieskuteczne

w tych państwach członkowskich, które nie stosowałyby się do zaleceń Komisji dotyczących budowy zdolności w obszarze bezpieczeństwa sieci i informacji.

Skutki gospodarcze: Tempo rozwoju różniłoby się znacznie w poszczególnych państwach członkowskich. Niedostateczny poziom bezpieczeństwa w mniej rozwiniętych państwach członkowskich prowadziłby do pogorszenia ich konkurencyjności oraz perspektyw wzrostu gospodarczego, narażając je na negatywne skutki incydentów i zagrożeń.

Skutki społeczne: Utrzymywanie się, a prawdopodobnie nawet nasilenie incydentów i zagrożeń miałoby negatywny wpływ na zaufanie do środowiska internetowego, zwłaszcza w tych państwach członkowskich, dla których bezpieczeństwo sieci i informacji nie stanowi priorytetu.

9. PORÓWNANIE WARIANTÓW

Warianty nr 1 i 3 uznaje się za nieodpowiednie dla osiągnięcia celów politycznych i w związku z tym nie są one zalecane, gdyż ich efektywność byłaby uzależniona od tego, czy podejście oparte na dobrowolności byłoby w stanie faktycznie doprowadzić do osiągnięcia minimalnego poziomu bezpieczeństwa sieci i informacji, a w przypadku wariantu nr 3 byłoby poza tym uzależnione od chęci budowy zdolności i prowadzenia współpracy transgranicznej przez państwa członkowskie.

Wariant nr 2 stanowi wariant preferowany, zważywszy że dzięki niemu możliwe byłoby istotne zwiększenie poziomu ochrony konsumentów, przedsiębiorstw i administracji publicznych w UE przed incydentami i zagrożeniami w obszarze bezpieczeństwa sieci i informacji. Ponadto uporządkowanie sytuacji u siebie umożliwiłoby UE zwiększenie swojego wpływu na arenie międzynarodowej i mogłaby się ona stać jeszcze bardziej wiarygodnym partnerem we współpracy na szczeblu dwu- i wielostronnym. Unia Europejska byłaby również w stanie lepiej promować za granicą prawa podstawowe i fundamentalne wartości UE.

10. MONITOROWANIE I OCENA

W rozdziale 10 sprawozdania z oceny skutków przedstawiono szereg podstawowych wskaźników służących ocenie postępu w osiągnięciu wyznaczonych celów. Wskaźniki te obejmują przykładowo:

- w odniesieniu do celu nr 1 – liczbę państw członkowskich, które wyznaczyły właściwy organ ds. bezpieczeństwa sieci i informacji oraz utworzyły zespół reagowania na incydenty komputerowe lub które przyjęły krajową strategię bezpieczeństwa cybernetycznego oraz krajowy plan awaryjny na wypadek incydentów cybernetycznych;
- w odniesieniu do celu nr 2 – liczbę właściwych organów państw członkowskich oraz zespołów reagowania na incydenty komputerowe należących do europejskiej sieci oraz ilość i zakres informacji dotyczących incydentów i zagrożeń w zakresie bezpieczeństwa sieci i informacji wymienionych w ramach tej sieci;
- w odniesieniu do celu nr 3 – poziom inwestycji w bezpieczeństwo sieci i informacji dokonanych przez kluczowe podmioty sektora prywatnego i organy administracji publicznej oraz liczbę dokonanych zgłoszeń dotyczących incydentów o znacznych skutkach w zakresie bezpieczeństwa sieci i informacji.