P9_TA(2021)0286

Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę

Rezolucja Parlamentu Europejskiego z dnia 10 czerwca 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę (2021/2568(RSP))

(2022/C 67/08)

Parlament Europejski,

— uwzględniając wspólny komunikat Komisji oraz Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki bezpieczeństwa z dnia 16 grudnia 2020 r. pt. „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę" (JOIN (2020)0018),

— uwzględniając wniosek Komisji z dnia 16 grudnia 2020 r. dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 (COM(2020)0823),

— uwzględniając wniosek Komisji z dnia 24 września 2020 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 (COM(2020)0595),

— uwzględniając wniosek Komisji z dnia 12 września 2018 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji (COM(2018)0630),

— uwzględniając komunikat Komisji z dnia 19 lutego 2020 r. pt. „Kształtowanie cyfrowej przyszłości Europy" (COM(2020)0067),

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) ([1]),

— uwzględniając dyrektywę 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylającą dyrektywę 1999/5/WE ([2]),

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej ([3]),

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1290/2013 z dnia 11 grudnia 2013 r. ustanawiające zasady uczestnictwa i upowszechniania dla programu „Horyzont 2020" – programu ramowego w zakresie badań naukowych i innowacji (2014–2020) oraz uchylające rozporządzenie (WE) nr 1906/2006 ([4]),

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1291/2013 z dnia 11 grudnia 2013 r. ustanawiające „Horyzont 2020" – program ramowy w zakresie badań naukowych i innowacji (2014–2020) oraz uchylające decyzję nr 1982/2006/WE ([5]),

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240 ([6]),

([1]) Dz.U. L 151 z 7.6.2019, s. 15.
([2]) Dz.U. L 153 z 22.5.2014, s. 62.
([3]) Dz.U. L 321 z 17.12.2018, s. 36.
([4]) Dz.U. L 347 z 20.12.2013, s. 81.
([5]) Dz.U. L 347 z 20.12.2013, s. 104.
([6]) Dz.U. L 166 z 11.5.2021, s. 1.

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady 2010/40/UE z dnia 7 lipca 2010 r. w sprawie ram wdrażania inteligentnych systemów transportowych w obszarze transportu drogowego oraz interfejsów z innymi rodzajami transportu ([7]),

— uwzględniając budapesztańską Konwencję o cyberprzestępczości z dnia 23 listopada 2001 r. (ETS nr 185),

— uwzględniając swoją rezolucję z dnia 16 grudnia 2020 r. w sprawie nowej strategii dla europejskich MŚP ([8]),

— uwzględniając swoją rezolucję z dnia 25 marca 2021 r. w sprawie europejskiej strategii w zakresie danych ([9]),

— uwzględniając swoją rezolucję z dnia 20 maja 2021 r. w sprawie kształtowania cyfrowej przyszłości Europy: usunięcie barier w funkcjonowaniu jednolitego rynku cyfrowego i lepsze wykorzystywanie AI z korzyścią dla europejskich konsumentów ([10]),

— uwzględniając swoją rezolucję z dnia 21 stycznia 2021 r. w sprawie zniwelowania przepaści cyfrowej między kobietami a mężczyznami: kobiety w sektorze cyfrowym ([11]),

— uwzględniając swoją rezolucję z dnia 12 marca 2019 r. w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia ([12]),

— uwzględniając pytanie do Komisji w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę (O-000037/2021 – B9-0024/2021),

— uwzględniając art. 136 ust. 5 i art. 132 ust. 2 Regulaminu,

A. mając na uwadze, że transformacja cyfrowa jest kluczowym priorytetem strategicznym Unii, który nieuchronnie wiąże się z większym narażeniem na zagrożenia dla cyberbezpieczeństwa;

B. mając na uwadze, że liczba urządzeń podłączonych do internetu, w tym maszyn, czujników, komponentów przemysłowych i sieci tworzących internet rzeczy, nadal rośnie – oczekuje się, że do 2024 r. z internetem rzeczy na całym świecie będzie połączonych 22,3 mld urządzeń, co zwiększy narażenie na cyberataki;

C. mając na uwadze, że postęp technologiczny – np. informatyka kwantowa – oraz asymetrie w dostępie do tych technologii mogą stanowić wyzwanie dla krajobrazu cyberbezpieczeństwa;

D. mając na uwadze, że kryzys związany z COVID-19 jeszcze bardziej ujawnił podatność na zagrożenia w cyberprzestrzeni w niektórych krytycznych sektorach, w szczególności w sektorze opieki zdrowotnej, a związane z kryzysem środki telepracy i ograniczenia kontaktów personalnych zwiększyły naszą zależność od technologii cyfrowych i łączności, podczas gdy w całej Europie coraz częściej odnotowuje się coraz bardziej wyrafinowane cyberataki i cyberprzestępczość, w tym szpiegostwo i sabotaż, a także wdzieranie się do systemów, struktur i sieci ICT oraz manipulowanie nimi za pomocą złośliwych i nielegalnych instalacji;

E. mając na uwadze, że liczba cyberataków znacznie wzrasta, jak pokazała niedawna seria szkodliwych i zorganizowanych cyberataków na systemy opieki zdrowotnej, np. w Irlandii, Finlandii i Francji; mając na uwadze, że cyberataki te powodują znaczne szkody dla systemów opieki zdrowotnej i opieki nad pacjentami, a także dla innych newralgicznych instytucji publicznych i prywatnych;

F. mając na uwadze, że zagrożenia hybrydowe, w tym stosowanie kampanii dezinformacyjnych i cyberataki na infrastrukturę, procesy gospodarcze i instytucje demokratyczne, są coraz liczniejsze i stają się poważnym problemem zarówno w cyberprzestrzeni, jak i w świecie fizycznym, i mogą mieć wpływ na procesy demokratyczne, takie jak wybory, procedury ustawodawcze, egzekwowanie prawa i wymiar sprawiedliwości;

G. mając na uwadze, że rośnie zależność od podstawowej funkcji internetu i podstawowych usług internetowych w zakresie komunikacji i hostingu, aplikacji i danych, w przypadku których to usług dochodzi stopniowo do koncentracji udziału w rynku w rękach coraz mniejszej liczby przedsiębiorstw;

([7]) Dz.U. L 207 z 6.8.2010, s. 1.
([8]) Teksty przyjęte, P9_TA(2020)0359.
([9]) Teksty przyjęte, P9_TA(2021)0098.
([10]) Teksty przyjęte, P9_TA(2021)0261.
([11]) Teksty przyjęte, P9_TA(2021)0026.
([12]) Dz.U. C 23 z 21.1.2021, s. 2.

H. mając na uwadze, że rozwijają się zdolności w zakresie rozproszonego ataku typu „odmowa usługi", w związku z czym należy równocześnie zwiększyć odporność rdzenia internetu;

I. mając na uwadze, że gotowość i świadomość w zakresie cyberbezpieczeństwa wśród przedsiębiorstw, w szczególności MŚP, i osób fizycznych utrzymuje się na niskim poziomie i istnieje niedobór wykwalifikowanych pracowników (niedostatek siły roboczej wzrósł o 20 % od 2015 r.), a tradycyjne kanały rekrutacji nie zaspokajają zapotrzebowania, w tym na stanowiska kierownicze i interdyscyplinarne; mając na uwadze, że „niemal 90 % pracowników w dziedzinie cyberbezpieczeństwa na świecie to mężczyźni" oraz że „utrzymujący się brak zróżnicowania płciowego w dalszej mierze ogranicza napływ utalentowanych osób" ([13]);

J. mając na uwadze, że zdolności państw członkowskich w zakresie cyberbezpieczeństwa są różne, a zgłaszanie incydentów i wymiana informacji między nimi nie są ani systematyczne, ani kompleksowe i nie wykorzystuje się wystarczająco ośrodków wymiany i analizy informacji (ISAC) do celów wymiany informacji między sektorem publicznym a prywatnym;

K. mając na uwadze, że na szczeblu UE brakuje porozumienia w sprawie współpracy w zakresie cyberwywiadu i zbiorowego reagowania na cyberataki i ataki hybrydowe; mając na uwadze, że państwom członkowskim bardzo trudno, z technicznego i geopolitycznego punktu widzenia, samodzielnie wprowadzać środki zaradcze przeciwko zagrożeniom dla cyberbezpieczeństwa i cyberatakom, zwłaszcza tym o charakterze hybrydowym;

L. mając na uwadze, że transgraniczna wymiana danych i globalna wymiana danych mają istotne znaczenie dla tworzenia wartości, pod warunkiem zagwarantowania prywatności oraz praw własności intelektualnej i praw własności; mając na uwadze, że egzekwowanie zagranicznych przepisów dotyczących danych może stanowić zagrożenie dla cyberbezpieczeństwa danych europejskich, ponieważ przedsiębiorstwa działające w różnych regionach podlegają nakładającym się na siebie obowiązkom niezależnie od lokalizacji danych lub ich pochodzenia;

M. mając na uwadze, że cyberbezpieczeństwo stanowi światowy rynek o wartości 600 mld EUR, przy czym oczekuje się, że kwota ta szybko wzrośnie, a Unia jest importerem netto produktów i rozwiązań;

N. mając na uwadze, że istnieje ryzyko fragmentacji jednolitego rynku ze względu na krajowe przepisy dotyczące cyberbezpieczeństwa oraz brak przepisów horyzontalnych dotyczących podstawowych wymogów cyberbezpieczeństwa w odniesieniu do sprzętu i oprogramowania, w tym produktów podłączonych do internetu i aplikacji;

1. z zadowoleniem przyjmuje inicjatywy przedstawione przez Komisję we wspólnym komunikacie zatytułowanym „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę";

2. wzywa do promowania rozwoju bezpiecznych i niezawodnych sieci i systemów informacyjnych oraz infrastruktury i połączeń w całej Unii;

3. wzywa do wyznaczenia celu, zgodnie z którym wszystkie produkty podłączone do internetu w Unii, w tym do użytku konsumenckiego i przemysłowego, wraz z całymi łańcuchami dostaw, które je udostępniają, muszą być zabezpieczane na etapie projektowania, odporne na cyberincydenty i szybko korygowane po wykryciu podatności na zagrożenia; z zadowoleniem przyjmuje, że Komisja planuje zaproponować horyzontalne przepisy dotyczące wymogów w zakresie cyberbezpieczeństwa w odniesieniu do produktów skomunikowanych i powiązanych usług, oraz wzywa do zaproponowania w tych przepisach harmonizacji przepisów krajowych w celu uniknięcia fragmentacji jednolitego rynku; domaga się, aby uwzględnić istniejące prawodawstwo (akt o cyberbezpieczeństwie, nowe ramy prawne, rozporządzenie w sprawie normalizacji) w celu uniknięcia niejasności i fragmentacji;

4. wzywa Komisję, by oceniła, czy do 2023 r. należy przedstawić wniosek dotyczący rozporządzenia horyzontalnego wprowadzającego wymogi w zakresie cyberbezpieczeństwa w odniesieniu do aplikacji, oprogramowania, oprogramowania wbudowanego i systemów operacyjnych, w oparciu o dorobek prawny UE dotyczący wymogów w zakresie zarządzania ryzykiem; podkreśla, że przestarzałe aplikacje, oprogramowanie, wbudowane oprogramowanie i systemy operacyjne (tj. nieotrzymujące już regularnych korekt i aktualizacji zabezpieczeń) stanowią istotną część wszystkich podłączonych do internetu urządzeń, a także zagrożenie dla cyberbezpieczeństwa; wzywa Komisję, aby uwzględniła ten aspekt w swoim wniosku; sugeruje, aby wniosek zawierał zobowiązanie producentów do informowania z wyprzedzeniem o minimalnym okresie, w którym będą proponować poprawki i aktualizacje zabezpieczeń, aby umożliwić nabywcom dokonywanie świadomych wyborów; uważa, że producenci muszą uczestniczyć w programie skoordynowanego ujawniania podatności określonego we wniosku dotyczącym dyrektywy NIS2;

([13]) Europejski Trybunał Obrachunkowy „Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją", dokument analityczny, marzec 2019 r.

5. podkreśla, że cyberbezpieczeństwo powinno być osadzone w cyfryzacji; w związku z tym apeluje, aby projekty cyfryzacji finansowane przez Unię obejmowały wymogi w zakresie cyberbezpieczeństwa; z zadowoleniem przyjmuje wsparcie badań naukowych i innowacji w dziedzinie cyberbezpieczeństwa, zwłaszcza w odniesieniu do przełomowych technologii (takich jak informatyka kwantowa i kryptografia kwantowa), których pojawienie się może zdestabilizować równowagę międzynarodową; wzywa ponadto do dalszych badań nad algorytmami postkwantowymi jako standardami cyberbezpieczeństwa;

6. uważa, że cyfryzacja naszego społeczeństwa oznacza, iż wszystkie sektory są ze sobą powiązane, a słabości jednego sektora mogą rzutować na inne sektory; nalega zatem, aby strategie cyberbezpieczeństwa zostały włączone do strategii cyfrowej UE i unijnego finansowania oraz aby były spójne i interoperacyjne we wszystkich sektorach;

7. wzywa do spójnego wykorzystania funduszy UE w odniesieniu do cyberbezpieczeństwa i rozmieszczenia odnośnej infrastruktury; wzywa Komisję i państwa członkowskie, by zapewniły wykorzystanie związanych z cyberbezpieczeństwem synergii między różnymi programami, w szczególności programami: „Horyzont Europa", „Cyfrowa Europa", unijny program kosmiczny, unijny Instrument na rzecz Odbudowy i Zwiększania Odporności, InvestEU i instrument „Łącząc Europę", a także by w pełni wykorzystywały centrum i sieć kompetencji w dziedzinie cyberbezpieczeństwa;

8. uważa, że infrastruktura komunikacyjna jest podstawą wszystkich działań cyfrowych oraz że zapewnienie jej bezpieczeństwa jest strategicznym priorytetem Unii; popiera obecny rozwój unijnego programu certyfikacji cyberbezpieczeństwa dla sieci 5G; z zadowoleniem przyjmuje unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa 5G i zachęca Komisję, państwa członkowskie i podmioty branży przemysłowej do kontynuowania wysiłków na rzecz bezpiecznych sieci komunikacyjnych, w tym środków dotyczących całego łańcucha dostaw; wzywa Komisję do unikania uzależnienia od jednego dostawcy i do zwiększenia bezpieczeństwa sieci poprzez promowanie inicjatyw zwiększających wirtualizację i „uchmurowienie" różnych komponentów sieci; wzywa do szybkiego opracowania nowych generacji technologii komunikacyjnych, których podstawową zasadą będzie uwzględnianie cyberbezpieczeństwa na etapie projektowania i które będą zapewniać ochronę prywatności i danych osobowych;

9. podkreśla, jak ważne jest ustanowienie nowych, solidnych ram bezpieczeństwa dla infrastruktury krytycznej UE, aby zabezpieczyć interesy UE w zakresie bezpieczeństwa i wykorzystać istniejące zdolności do odpowiedniego reagowania na ryzyko, zagrożenia i zmiany technologiczne;

10. wzywa Komisję do przygotowania przepisów zapewniających dostępność i integralność publicznego rdzenia internetu, a tym samym stabilność cyberprzestrzeni, w szczególności w odniesieniu do dostępu UE do globalnego systemu serwerów DNS; uważa, że takie przepisy powinny obejmować środki na rzecz dywersyfikacji dostawców w celu ograniczenia obecnego ryzyka uzależnienia od niewielu przedsiębiorstw, które dominują na rynku; z zadowoleniem przyjmuje wniosek dotyczący europejskiego systemu nazw domen (DNS4EU) jako narzędzia służącego zwiększeniu odporności rdzenia internetu; zwraca się do Komisji o dokonanie oceny, w jaki sposób w ramach DNS4EU można by wykorzystać najnowsze technologie, protokoły bezpieczeństwa i wiedzę fachową o zagrożeniach dla cyberbezpieczeństwa w celu zaoferowania wszystkim Europejczykom szybkiego, bezpiecznego i odpornego DNS; przypomina o konieczności lepszej ochrony zewnętrznego protokołu trasowania (Border Gateway Protocol, BGP), aby zapobiec jego piratowaniu; przypomina, że popiera wielostronny model zarządzania internetem i że jednym z głównych jego elementów powinno być cyberbezpieczeństwo; podkreśla, że UE powinna przyspieszyć wdrażanie IPv6; uznaje model otwartego oprogramowania, który jako podstawa funkcjonowania internetu okazał się wydajny i skuteczny; w związku z tym zachęca do korzystania z niego;

11. uznaje potrzebę rozwijania kryminalistyki w zakresie cyberbezpieczeństwa w celu zwalczania przestępczości, cyberprzestępczości i cyberataków, w tym ataków wspieranych przez państwa, ale ostrzega przed nieproporcjonalnymi środkami, które zagrażają prywatności i wolności słowa obywateli UE korzystających z internetu; przypomina, że trzeba zakończyć przegląd drugiego protokołu dodatkowego do budapeszteńskiej Konwencji o cyberprzestępczości, który może zwiększyć gotowość do zwalczania cyberprzestępczości;

12. wzywa Komisję i państwa członkowskie do połączenia zasobów w celu zwiększenia odporności strategicznej UE, zmniejszenia jej zależności od technologii zagranicznych oraz wzmocnienia jej wiodącej pozycji i konkurencyjności w zakresie cyberbezpieczeństwa w całym cyfrowym łańcuchu dostaw (w tym jeśli chodzi o przechowywanie i przetwarzanie danych w chmurze, technologie procesorów, układy scalone (chipy), wysoce bezpieczne połączenia, informatykę kwantową i sieci nowej generacji);

13. uważa, że plan dotyczący wysoce bezpiecznej infrastruktury łączności jest ważnym instrumentem na potrzeby bezpieczeństwa newralgicznej komunikacji cyfrowej; z zadowoleniem przyjmuje zapowiedź opracowania unijnego systemu globalnej bezpiecznej komunikacji satelitarnej obejmującego technologie szyfrowania kwantowego; przypomina, że należy podejmować stałe wysiłki, we współpracy z Agencją Unii Europejskiej ds. Programu Kosmicznego (EUSPA) i Europejską Agencją Kosmiczną (ESA), w celu zabezpieczenia europejskich działań związanych z przestrzenią kosmiczną;

14. ubolewa, że praktyki wymiany informacji dotyczących zagrożeń dla cyberbezpieczeństwa i cyberincydentów nie zostały dobrze przyjęte przez sektor prywatny i publiczny; wzywa Komisję i państwa członkowskie do zwiększenia zaufania i ograniczenia barier w wymianie informacji na temat zagrożeń dla cyberbezpieczeństwa i cyberataków na wszystkich szczeblach; z zadowoleniem przyjmuje wysiłki podejmowane przez niektóre sektory i wzywa do współpracy międzysektorowej, ponieważ podatności na zagrożenia rzadko dotyczą konkretnych sektorów; podkreśla, że państwa członkowskie muszą połączyć siły na szczeblu europejskim, aby skutecznie dzielić się najnowszymi informacjami na temat zagrożeń dla cyberbezpieczeństwa; zachęca do utworzenia grupy roboczej państw członkowskich ds. cyberwywiadu w celu wspierania wymiany informacji w UE i w europejskiej przestrzeni gospodarczej, w szczególności aby zapobiegać cyberatakom na dużą skalę;

15. z zadowoleniem przyjmuje planowane utworzenie wspólnej jednostki ds. cyberprzestrzeni w celu zacieśnienia współpracy między organami UE i organami państw członkowskich odpowiedzialnymi za zapobieganie cyberatakom, powstrzymywanie ich i reagowanie na nie; wzywa państwa członkowskie i Komisję do dalszego zacieśniania współpracy w dziedzinie cyberobrony i rozwijania badań nad najnowocześniejszymi zdolnościami w zakresie cyberobrony;

16. przypomina, jak ważny w strategii cyberbezpieczeństwa jest czynnik ludzki; wzywa do dalszych wysiłków na rzecz rozpowszechniania wiedzy na temat cyberbezpieczeństwa, w tym higieny cyberbezpieczeństwa i umiejętności cyfrowych;

17. podkreśla, jak ważne są solidne i spójne ramy bezpieczeństwa dla ochrony wszystkich pracowników, danych, sieci komunikacyjnych i systemów informacyjnych UE oraz procesów decyzyjnych przed zagrożeniami dla cyberbezpieczeństwa w oparciu o kompleksowe, spójne i jednolite przepisy oraz odpowiednie zarządzanie; wzywa do udostępnienia wystarczających zasobów i zdolności, w tym w kontekście wzmocnienia mandatu CERT-UE oraz w odniesieniu do toczących się dyskusji na temat określenia wspólnych wiążących zasad cyberbezpieczeństwa dla wszystkich instytucji, organów i agencji UE;

18. wzywa do szerszego stosowania dobrowolnych standardów w zakresie certyfikacji i cyberbezpieczeństwa, ponieważ są to ważne narzędzia służące poprawie ogólnego poziomu cyberbezpieczeństwa; z zadowoleniem przyjmuje ustanowienie europejskich ram certyfikacji oraz prace Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa; wzywa ENISA i Komisję, aby podczas przygotowywania unijnego programu certyfikacji cyberbezpieczeństwa dla usług w chmurze rozważyły wprowadzenie obowiązku stosowania prawa UE w odniesieniu do „wysokiego" poziomu bezpieczeństwa;

19. podkreśla, że należy zaspokoić popyt na pracę w dziedzinie cyberbezpieczeństwa oraz zlikwidować lukę kompetencyjną poprzez kontynuowanie wysiłków na rzecz kształcenia i szkolenia; wzywa do zwrócenia szczególnej uwagi na wyeliminowanie różnic w traktowaniu kobiet i mężczyzn, które występują również w tym sektorze;

20. uważa, że należy w większym stopniu wspierać mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, aby lepiej zrozumiały wszystkie zagrożenia związane z bezpieczeństwem informacji i mogły poprawić swoje cyberbezpieczeństwo; wzywa ENISA i organy krajowe do opracowania portali samotestujących i przewodników najlepszych praktyk dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw; przypomina o znaczeniu, jakie dla bezpieczeństwa tych podmiotów mają szkolenia i dostęp do specjalnego finansowania;

21. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Komisji i Radzie oraz rządom i parlamentom państw członkowskich.