



Komunikat prasowy

Luksemburg, 17 grudnia 2020 r.

Organy kontroli w UE wspólnie publikują wyniki prac dotyczących cyberbezpieczeństwa

W miarę jak w ostatnich latach rośnie zagrożenie cyberprzestępczością i cyberatakami, kontrolerzy w całej UE z coraz większą uwagą przyglądali się odporności systemów informatycznych i infrastruktury cyfrowej o krytycznym znaczeniu. Komitet Kontaktowy zrzeszający najwyższe organy kontroli (NOK) w UE opublikował dzisiaj kompendium kontroli na temat cyberbezpieczeństwa, w którym przedstawił przegląd prac kontrolnych przeprowadzonych w tym obszarze przez NOK.

Cyberincydenty mogą zostać wywołane umyślnie lub nieumyślnie. Obejmują one różnorodne wydarzenia, począwszy od niezamierzonego ujawnienia informacji po ataki na przedsiębiorstwa i infrastrukturę krytyczną, kradzież danych osobowych, a nawet przypadki zakłócenia przebiegu procesów demokratycznych, w tym wyborów, oraz ogólne kampanie dezinformacyjne mające wpłynąć na debatę publiczną. Już przed wybuchem pandemii COVID-19 cyberbezpieczeństwo stanowiło sprawę wielkiej wagi dla obywateli UE, a wskutek pandemii, z której konsekwencjami mierzy się obecnie UE, cyberzagrożenia będą problemem na jeszcze większą skalę. Wiele przedsiębiorstw i instytucji publicznych zrezygnowało bowiem z pracy w biurach na rzecz pracy zdalnej. Jednocześnie fałszywe informacje i teorie spiskowe szerzą się z niespotykaną dotąd siłą.

Zabezpieczenie krytycznych systemów informatycznych i infrastruktury cyfrowej przed cyberatakami staje się w związku z tym coraz istotniejszym wyzwaniem strategicznym, przed którym stoją UE i państwa członkowskie. Pytanie, które należy sobie postawić, nie dotyczy już tego, czy cyberataki będą miały miejsce, ale w jaki sposób i kiedy zostaną przeprowadzone.

Niniejszy komunikat prasowy stanowi streszczenie kompendium kontroli opracowanego przez [Komitet Kontaktowy](#) zrzeszający najwyższe organy kontroli w UE i Europejski Trybunał Obrachunkowy.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

E: press@eca.europa.eu @EUAuditors eca.europa.eu

Zagrożenie to dotyczy wszystkich – tak osób prywatnych, jak i przedsiębiorstw oraz instytucji publicznych.

– Kryzys związany z pandemią COVID-19 stał się sprawdzianem dla gospodarczej i społecznej konstrukcji naszego społeczeństwa. Jesteśmy tak zależni od technologii informacyjnych, że cyberkryzys może okazać się dla nas takim zagrożeniem jak kolejna pandemia – **powiedział Klaus-Heiner Lehne, prezes Europejskiego Trybunału Obrachunkowego**. – Nie ma wątpliwości, że w najbliższej dekadzie dążenie do autonomii cyfrowej i mierzenie się z wyzwaniami, jakie niosą za sobą cyberzagrożenia i zewnętrzne kampanie dezinformacyjne, nadal będą częścią naszej codzienności i pozostaną wśród politycznych priorytetów. Dlatego właśnie tak ważne jest informowanie o ustaleniach poczynionych w toku kontroli dotyczących cyberbezpieczeństwa, które zostały przeprowadzone w ostatnim czasie w państwach członkowskich UE.

W ubiegłych latach najwyższe organy kontroli w UE zintensyfikowały prace kontrolne w zakresie cyberbezpieczeństwa. Kontrolerzy położyli szczególny nacisk na kwestię ochrony danych, gotowość systemów na cyberataki oraz zabezpieczenie systemów zapewniających najważniejsze usługi użyteczności publicznej. Pod uwagę wzięli także ambicję UE, by stworzyć najbezpieczniejsze środowisko cyfrowe na świecie. Komisja Europejska i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawili w ostatnich dniach nową [unijną strategię na rzecz cyberbezpieczeństwa](#), której celem jest wzmocnienie zbiorowej odporności europejskiej na cyberzagrożenia.

W opublikowanym dzisiaj kompendium przedstawiono informacje na temat cyberbezpieczeństwa, głównych inicjatyw strategicznych oraz podstaw prawnych obowiązujących w tej dziedzinie w UE. Ukazano także najistotniejsze wyzwania stojące przed UE i państwami członkowskimi, takie jak zagrożenia dla praw obywateli UE spowodowane niewłaściwym wykorzystaniem danych osobowych czy ryzyko, że w następstwie cyberataku instytucje nie będą w stanie świadczyć kluczowych usług publicznych bądź będą mogły je świadczyć jedynie w ograniczonym zakresie.

W kompendium przedstawiono wyniki kontroli przeprowadzonych przez Europejski Trybunał Obrachunkowy i najwyższe organy kontroli z 12 państw członkowskich UE: Danii, Estonii, Irlandii, Francji, Łotwy, Litwy, Węgier, Niderlandów, Polski, Portugalii, Finlandii i Szwecji.

Informacje ogólne

Kompendium kontroli jest efektem współpracy między krajowymi NOK i Europejskim Trybunałem Obrachunkowym w ramach Komitetu Kontaktowego UE. Zostało ono pomyślane jako źródło informacji dla osób zainteresowanych tym ważnym obszarem polityki. Obecnie publikacja dostępna jest w j. angielskim na [stronie internetowej Komitetu Kontaktowego](#). Wkrótce dokument ukaże się także w innych językach UE.

Ukazująca się właśnie publikacja to trzecie kompendium kontroli przygotowane przez Komitet Kontaktowy. Pierwsze kompendium – na temat [bezrobocia młodzieży i integracji ludzi młodych na rynku pracy](#) – zostało opublikowane w czerwcu 2018 r. Drugie kompendium dotyczyło [zdrowia publicznego w UE](#) i ukazało się w grudniu 2019 r.

Komitet Kontaktowy jest autonomicznym i niezależnym zgromadzeniem o charakterze niepolitycznym, które zrzesza prezesów NOK państw członkowskich i Europejskiego Trybunału Obrachunkowego. Stanowi forum, na którym omawiane i rozpatrywane są kwestie związane

z UE, będące przedmiotem wspólnego zainteresowania. Poprzez wspieranie dialogu i zacieśnianie współpracy między swoimi członkami Komitet Kontaktowy wnosi istotny wkład w skuteczną i niezależną kontrolę zewnętrzną polityki i programów UE.

Kontakt dla prasy

Vincent Bourgeais – e-mail: vincent.bourgeais@eca.europa.eu

Tel.: (+352) 4398 47502 / tel. kom.: (+352) 691 551 502