EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY

PL

Komunikat prasowy

Luksemburg, 29 marca 2022 r.

Instytucje unijne muszą być lepiej przygotowane do obrony przed cyberatakami

Liczba cyberataków na instytucje unijne gwałtownie rośnie. Instytucje te są jednak nierównomiernie przygotowane do ich odpierania, a ogólny poziom zabezpieczeń unijnych jest nieadekwatny do zagrożeń. Ze względu na ścisłe powiązania między instytucjami luki w zabezpieczeniach w jednej z nich mogą zagrażać bezpieczeństwu pozostałych. Europejski Trybunał Obrachunkowy zbadał, jak instytucje kierujące Unią są przygotowane na sprostanie cyberzagrożeniom. W sprawozdaniu specjalnym kontrolerzy zalecają, aby przyjąć wiążące zasady cyberbezpieczeństwa oraz udostępnić większe zasoby zespołowi reagowania na incydenty komputerowe (CERT-UE). Stwierdzili też, że Komisja Europejska powinna zadbać o lepszą współpracę między organami UE, a CERT-UE i Agencja Unii Europejskiej ds. Cyberbezpieczeństwa – poświęcić więcej uwagi tym instytucjom, które mają mniej doświadczenia w tej dziedzinie.

W latach 2018–2021 liczba istotnych cyberincydentów w instytucjach unijnych zwiększyła się ponad dziesięciokrotnie, a ze względu na upowszechnienie się pracy zdalnej możliwych dróg ataku jest o wiele więcej. Istotny cyberincydent jest zazwyczaj rezultatem złożonego cyberataku, najczęściej dokonanego z wykorzystaniem nowych metod i technologii. Przeprowadzenie dochodzenia i wyeliminowanie skutków może zająć wiele tygodni, o ile nie miesięcy. Jednym z przykładów takiego cyberincydentu był atak na Europejską Agencję Leków. Doszło do wycieku danych wrażliwych, które zmanipulowano w celu podważenia zaufania do szczepionek.

– Instytucje, organy i agencje UE są atrakcyjnym celem dla potencjalnych atakujących, zwłaszcza dla grup, które w ramach cyberszpiegostwa lub działalności przestępczej przeprowadzają misternie zaplanowane ataki z ukrycia – stwierdziła Bettina Jakobsen, członkini Trybunału odpowiedzialna za tę kontrolę. – Te ataki mogą mieć poważne konsekwencje polityczne, zaszkodzić ogólnej reputacji UE i podważyć zaufanie do instytucji unijnych – dodała członkini Trybunału i zaznaczyła, że UE musi dołożyć większych starań, aby chronić swoje instytucje.

Kontrolerzy ustalili przede wszystkim, że instytucje, organy i agencje UE nie zawsze są dobrze przygotowane do odparcia cyberzagrożeń. Nie mają one spójnego podejścia do cyberbezpieczeństwa, nie wszystkie też wprowadziły podstawowe środki bezpieczeństwa, stosowały kluczowe dobre praktyki i zapewniały regularne szkolenia. Przydział zasobów na

Niniejszy komunikat prasowy stanowi streszczenie sprawozdania specjalnego przyjętego przez Europejski Trybunał Obrachunkowy. Pełny tekst sprawozdania dostępny jest na stronie eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

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

cyberbezpieczeństwo w poszczególnych instytucjach unijnych jest bardzo zróżnicowany, a wiele z nich wydaje na ten cel znacznie mniej niż porównywalne z nimi organizacje. Różnice w poziomie cyberbezpieczeństwa w instytucjach można by teoretycznie uzasadnić zróżnicowaniem profilów ryzyka i przetwarzanych przez nie danych wrażliwych. Kontrolerzy podkreślają jednak, że luki w zabezpieczeniach w jednej z instytucji mogą narazić na zagrożenie wiele innych (wszystkie instytucje unijne są powiązane między sobą, a często także z podmiotami publicznymi i prywatnymi w państwach członkowskich).

Zespół reagowania na incydenty komputerowe (CERT-UE) i Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) to dwa najważniejsze podmioty unijne, których zadaniem jest udzielanie wsparcia w obszarze cyberbezpieczeństwa. Nie były one jednak w stanie zapewnić instytucjom unijnym potrzebnej pomocy ze względu na ograniczone zasoby oraz dlatego, że za priorytetowe uznano inne obszary działania. Zdaniem kontrolerów niedostateczna jest też wymiana informacji. Przykładowo nie wszystkie instytucje przekazują na czas informacje o lukach w zabezpieczeniach i istotnych cyberincydentach, które mają wpływ na ich pracę i mogą dotknąć inne instytucje.

Informacje ogólne

Nie ma obecnie ram prawnych, które regulowałyby bezpieczeństwo informacji i cyberbezpieczeństwo w instytucjach, agencjach i organach UE. Nie podlegają one podstawowemu prawodawstwu UE w dziedzinie cyberbezpieczeństwa, tj. dyrektywie w sprawie bezpieczeństwa sieci i informacji z 2016 r. (tzw. dyrektywie NIS), ani nie mają podlegać jej proponowanej zmienionej wersji (dyrektywie NIS 2). Brakuje również kompleksowych informacji na temat wydatków instytucji na cyberbezpieczeństwo. Wspólne przepisy obowiązujące wszystkie instytucje unijne zawarto w komunikacie w sprawie strategii UE w zakresie unii bezpieczeństwa na lata 2020–2025, opublikowanym przez Komisję w lipcu 2020 r. W strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę z grudnia 2020 r. Komisja zobowiązała się do przedstawienia wniosku dotyczącego rozporządzenia w sprawie wspólnych zasad cyberbezpieczeństwa dla wszystkich instytucji unijnych. Zaproponowała w niej również ustanowienie nowej podstawy prawnej dla CERT-UE w celu wzmocnienia jego mandatu i zwiększenia finansowania.

Sprawozdanie specjalne nr 5/2022 pt. „Cyberbezpieczeństwo instytucji, organów i agencji UE – poziom przygotowania ogólnie nieadekwatny do zagrożeń” jest dostępne na stronie internetowej Trybunału. Wyzwania na drodze do skutecznej realizacji unijnej polityki cyberbezpieczeństwa Trybunał przedstawił ponadto w przeglądzie z 2019 r.

Kontakt dla prasy

Biuro prasowe Trybunału: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu – tel. kom.: (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu – tel. kom.: (+352) 691 551 502
- Damijan Fišer – e-mail: damijan.fiser@eca.europa.eu – tel. kom.: (+352) 621 552 224