Unijne ćwiczenie w dziedzinie cyberbezpieczeństwa – zacieśnienie współpracy w celu wsparcia wolnych i uczciwych wyborów europejskich

Instytucje UE przeprowadziły wczoraj ćwiczenie w dziedzinie cyberbezpieczeństwa, które miało na celu ocenę i ulepszenie obecnych metod działania przed wyborami w 2024 r. Przetestowano plany kryzysowe oraz możliwe reakcje na potencjalne cyberincydenty mające wpływ na wybory europejskie.

Ćwiczenie to stanowi jeden ze środków wdrażanych przez Unię Europejską w celu zagwarantowania wolnych i uczciwych wyborów w czerwcu 2024 r. Odbyło się ono w Parlamencie Europejskim i zostało zorganizowane przez służby Parlamentu Europejskiego, Komisję Europejską i Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Ćwiczenie umożliwiło uczestnikom wymianę doświadczeń i najlepszych praktyk oraz pomogło im zwiększyć zdolności reagowania na cyberincydenty. Przyczyni się ono również do aktualizacji istniejących wytycznych i dobrych praktyk w zakresie cyberbezpieczeństwa technologii wykorzystywanych w procesie wyborczym.

W przeprowadzonym drugi raz ćwiczeniu uczestniczyli przedstawiciele krajowych organów wyborczych i krajowych organów ds. cyberbezpieczeństwa oraz obserwatorzy z Parlamentu Europejskiego, Komisji Europejskiej, Centrum ds. Cyberbezpieczeństwa instytucji, organów i agencji Unii (CERT-UE) oraz ENISA. Odpowiedzialność za zapewnienie uczciwości wyborów spoczywa zasadniczo na państwach członkowskich UE – ćwiczenie to pomogło ulepszyć ich wspólną gotowość w obliczu potencjalnych zagrożeń cybernetycznych i innych zagrożeń hybrydowych oraz ich zdolność do szybkiego rozwinięcia i utrzymania orientacji sytuacyjnej na szczeblu krajowym i unijnym w przypadku wystąpienia poważnego cyberincydentu.

Dołożono wszelkich starań, by obywatele europejscy mogli mieć zaufanie do procesu wyborczego w UE. Zagrożenia związane z wyborami mogą przybierać różne formy – od manipulacji informacjami i dezinformacji po cyberataki zagrażające infrastrukturze.

W oparciu o różne scenariusze obejmujące potencjalne zagrożenia cybernetyczne i cyberincydenty ćwiczenie umożliwiło uczestnikom:

- pogłębienie wiedzy na temat kluczowych aspektów wyborów europejskich, w tym oceny poziomu świadomości wśród innych zainteresowanych stron (np. partii politycznych, podmiotów organizujących kampanie wyborcze i dostawców odpowiedniego sprzętu informatycznego);
- zacieśnienie współpracy między właściwymi organami na szczeblu krajowym (w tym organami wyborczymi oraz innymi odpowiednimi organami i agencjami, takimi jak organy ds. cyberbezpieczeństwa, zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), organy ochrony danych, organy zajmujące się problemem dezinformacji itp.) oraz na szczeblu UE (takimi jak służby Komisji odpowiedzialne za egzekwowanie przepisów aktu o usługach cyfrowych);
- weryfikację istniejących zdolności państw członkowskich UE w zakresie adekwatnej oceny zagrożeń związanych z cyberbezpieczeństwem wyborów europejskich, szybkiego rozwijania orientacji sytuacyjnej i koordynowania komunikacji ze społeczeństwem;
- przetestowanie istniejących planów zarządzania kryzysowego, a także stosownych procedur zapobiegania atakom na cyberbezpieczeństwo i zagrożeniom hybrydowym (w tym kampaniom dezinformacyjnym), wykrywania takich ataków i zagrożeń oraz zarządzania nimi i reagowania na nie;
- zidentyfikowanie wszelkich innych potencjalnych luk oraz określenie adekwatnych środków ograniczających ryzyko, które należy wdrożyć przed wyborami do Parlamentu Europejskiego.

Dodatkowe informacje

Wybory do Parlamentu Europejskiego