EURÓPAI SZÁMVEVŐSZÉK

HU

Sajtóközlemény

Luxembourg, 2022. március 29.

Az uniós szerveknek javítaniuk kell kiberbiztonsági felkészültségüket

Meredeken nő az uniós szervek ellen elkövetett kibertámadások száma. Az uniós szervek kiberbiztonsági felkészültsége nem egységes és összességében nem áll arányban a fokozódó fenyegetettséggel. Mivel az uniós szervek szorosan kapcsolódnak egymáshoz, egyikük gyengeségei másokat is biztonsági kockázatoknak tehetnek ki. Erre a következtetésre jutott az Európai Számvevőszék ebben a különjelentésében, amely azt vizsgálja, mennyire felkészülten néznek szembe az Uniót irányító szervek a kibertámadásokkal. A számvevők kötelező érvényű kiberbiztonsági szabályok bevezetését és a hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT-EU) rendelkezésére álló források növelését javasolják. Emellett a számvevők szerint az Európai Uniónak ösztönöznie kellene az uniós szervek közötti együttműködés elmélyítését, a CERT-EU-nak és az Európai Uniós Kiberbiztonsági Ügynökségnek pedig több figyelmet kellene fordítania a kiberbiztonsági irányítás terén kevésbé tapasztalt uniós szervekre.

Az uniós szerveknél bekövetkezett jelentős kiberbiztonsági események száma 2018 és 2021 között több mint tízszeresére emelkedett; a távmunka miatt jelentősen megnőtt a támadók által kihasználható potenciális hozzáférési pontok száma. A jelentős biztonsági eseményeket általában összetett kibertámadások okozzák, amelyek jellemzően új módszereket és technológiákat alkalmaznak, így a kivizsgálás és a helyreállítás hetekbe vagy akár hónapokba telhet. Példa erre az Európai Gyógyszerügynökség elleni kibertámadás, amelynek során érzékeny adatokat szivárogtattak ki és manipuláltak oly módon, hogy az aláássa az oltásokba vetett bizalmat.

„Az uniós intézmények, szervek és ügynökségek vonzó célpontot jelentenek a potenciális támadók és különösen azon csoportok számára, amelyek kiberkémkedési és egyéb kártékony célokból képesek rendkívül kifinomult lopakodó támadásokat végrehajtani – jelentette ki Bettina Jakobsen, az ellenőrzést vezető számvevőszéki tag. – *Az ilyen támadásoknak akár súlyos politikai következményei is lehetnek, árthatnak az Unió általános megítélésének, és alááshatják az intézményekbe vetett bizalmat. Az Uniónak többet kell tennie saját szervezeteinek védelméért.”*

A számvevők elsősorban azt állapították meg, hogy az uniós intézmények, szervek és ügynökségek nem mindig élveznek kellő védelmet a kiberfenyegetésekkel szemben. Nem alkalmaznak egységes megközelítést a kiberbiztonság kérdését illetően, nem vezették be mindenütt a legfontosabb kiberbiztonsági kontrollokat és bevált gyakorlatokat, továbbá nem biztosítanak szisztematikusan képzéseket ezekben a témákban. Nagy különbségek vannak a kiberbiztonságra előirányzott

E sajtóközlemény célja, hogy összefoglalót nyújtson az Európai Számvevőszék által elfogadott különjelentésről. A jelentés teljes szövege letölthető a Számvevőszék honlapján (eca.europa.eu).

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg
E: press@eca.europa.eu @EUAuditors eca.europa.eu

források terén: néhány uniós szerv jóval kevesebbet költ ilyen célra, mint hasonló méretű társaik. Bár az eltérő kiberbiztonsági felkészültséget elvben indokolhatja, hogy a különböző szervezetek más-más kockázati profillal rendelkeznek és különféle érzékenységű adatokat kezelnek, a számvevők hangsúlyozzák, hogy mivel mind az uniós szervek között, mind azok és a tagállami köz- és magánszervezetek között sok a kapcsolódási pont, akár egyetlen uniós szerv kiberbiztonsági gyengeségei több más szervet is kiberfenyegetésnek tehetnek ki.

A kiberbiztonság támogatás nyújtásáért felelős két fő uniós szervezet az európai intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportja (CERT-EU) és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA). A korlátozott erőforrások, illetve más területek előnyben részesítése miatt azonban ezek nem voltak képesek megadni minden szükséges támogatást az uniós szerveknek. A számvevők szerint további problémát jelent az információk megosztása: nem minden uniós szerv számol be például kellő időben az általa elszenvedett, potenciálisan más szereplőket is fenyegető sebezhetőségekről és jelentős kiberbiztonsági eseményekről.

Háttér-információk

Jelenleg nincs hatályban olyan jogi keret, amely az uniós intézmények, szervek és ügynökségek információbiztonságát és kiberbiztonságát szabályozná. E szervekre nem terjed ki sem a kiberbiztonságra vonatkozó legáltalánosabb uniós jogszabálynak (a 2016. évi NIS-irányelvnek), sem pedig javasolt felülvizsgált változatának (NIS2) a hatálya. Arról sem áll rendelkezésre átfogó információ, hogy az uniós szervek mekkora összegeket költenek a kiberbiztonságra. A Bizottság 2020 júliusában közleményt tett közzé a biztonsági unióra vonatkozó, a 2020 és 2025 közötti időszakra érvényes uniós stratégiáról, amely foglalkozik a valamennyi uniós szerv által alkalmazandó, az információbiztonságra és a kiberbiztonságra vonatkozó közös szabályok meghatározásával is. Az Unió digitális évtizedre szóló kiberbiztonsági stratégiájában, amelyet 2020 decemberében tettek közzé, a Bizottság vállalta, hogy javaslatot tesz egy, az összes uniós szervre vonatkozó közös kiberbiztonsági szabályokról szóló rendeletre. Javasolta továbbá a CERT-EU új jogalapjának létrehozását a szervezet megbízatásának és finanszírozásának megerősítése érdekében.

„Az uniós intézmények, szervek és ügynökségek kiberbiztonsága: a felkészültség szintje összességében nem áll arányban a fenyegetésekkel” című, 05/2022. sz. különjelentés a Számvevőszék honlapján érhető el. A Számvevőszék már egy 2019-ben közzétett áttekintésben is rámutatott az eredményes uniós kiberbiztonsági politika előtt álló kihívásokra.

A sajtó rendelkezésére áll:

A Számvevőszék sajtóirodája: press@eca.europa.eu

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