2024/2690

2024.10.18.

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

(2024. október 17.)

az (EU) 2022/2555 irányelvnek a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményei, valamint a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események eseteinek további pontosítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvre [1] (NIS 2 irányelv) és különösen annak 21. cikke (5) bekezdése első albekezdésére, valamint 23. cikke (11) bekezdése második albekezdésére,

mivel:

(1) E rendelet célja, hogy az (EU) 2022/2555 irányelv 3. cikkének hatálya alá tartozó DNS-szolgáltatók, legfelső szintű doménnév-nyilvántartók, felhőszolgáltatók, adatközpont-szolgáltatók, tartalomszolgáltató hálózati szolgáltatók, irányított szolgáltatók, irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók (a továbbiakban: érintett szervezetek) tekintetében meghatározza az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésében említett intézkedések technikai és módszertani követelményeit, valamint hogy tovább pontosítsa azokat az eseteket, amelyekben egy biztonsági esemény az (EU) 2022/2555 irányelv 23. cikke (3) bekezdésének értelmében vett jelentős biztonsági eseménynek tekintendő.

(2) Figyelembe véve tevékenységeik határokon átnyúló jellegét, valamint a bizalmi szolgáltatók számára a koherens keretek megteremtése érdekében e rendeletnek a megbízható szolgáltatók tekintetében – a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményeinek meghatározása mellett – tovább kell pontosítania azokat az eseteket, amikor egy biztonsági eseményt jelentősnek kell tekinteni.

(3) Az (EU) 2022/2555 irányelv 21. cikke (5) bekezdésének harmadik albekezdésének megfelelően a kiberbiztonsági kockázatkezelési intézkedések e rendelet mellékletében meghatározott technikai és módszertani követelményei olyan európai és nemzetközi szabványokon alapulnak, mint az ISO/IEC 27001, az ISO/IEC 27002 és az ETSI EN 319401 szabvány, valamint a hálózati és információs rendszerek biztonsága szempontjából releváns műszaki előírások, például a CEN/TS 18026:2024.

(4) Ami az e rendelet mellékletében meghatározott kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményeinek végrehajtását és alkalmazását illeti, az arányosság elvével összhangban kellően figyelembe kell venni az érintett szervezetek eltérő kockázati kitettségét, például az érintett szervezet kritikusságát, a kockázatokat, amelyeknek a szervezet ki van téve, a szervezet méretét és szerkezetét, valamint a biztonsági események előfordulásának valószínűségét és súlyosságát, beleértve azok társadalmi és gazdasági hatását, amennyiben a szervezet megfelel a kiberbiztonsági kockázatkezelési intézkedések e rendelet mellékletében meghatározott technikai és módszertani követelményeinek.

[1] HL L 333., 2022.12.27., 80. o., ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) Az arányosság elvével összhangban, amennyiben az érintett szervezetek méretük miatt nem tudják végrehajtani a kiberbiztonsági kockázatkezelési intézkedések bizonyos technikai és módszertani követelményeit, e szervezetek számára lehetővé kell tenni, hogy az említett követelmények céljának elérésére alkalmas egyéb kompenzációs intézkedéseket hozzanak. Például az érintett szervezeten belüli hálózati és információs rendszer biztonságával kapcsolatos szerepkörök, felelősségi körök és hatóságok meghatározásakor a mikrovállalkozások számára nehézséget okozhat az összeférhetetlen feladatok és az összeférhetetlen felelősségi területek elkülönítése. Az ilyen szervezetek számára lehetővé kell tenni, hogy adott esetben kompenzációs intézkedéseket vezessenek be, például a szervezet vezetése általi célzott felügyeletet vagy fokozott nyomon követést és naplózást.

(6) Az e rendelet mellékletében meghatározott bizonyos technikai és módszertani követelményeket az érintett szervezeteknek akkor kell alkalmazniuk, ha indokolt, ha releváns vagy ha megvalósítható. Amennyiben az érintett szervezet úgy ítéli meg, hogy az e rendelet mellékletében előírt bizonyos technikai és módszertani követelmények alkalmazása nem indokolt, nem releváns vagy nem megvalósítható, az érintett szervezetnek érthető módon dokumentálnia kell az erre vonatkozó érvelését. Az illetékes nemzeti hatóságok a felügyelet gyakorlása során figyelembe vehetik az érintett szervezetek számára mennyi idő szükséges a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményeinek végrehajtásához.

(7) Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) vagy az (EU) 2022/2555 irányelv szerinti illetékes nemzeti hatóságok iránymutatásukkal támogathatják az érintett szervezeteket a kockázatoknak a megfelelő kockázatkezelési keret létrehozására és fenntartására vonatkozó technikai és módszertani követelmények végrehajtása céljából végzett azonosításában, elemzésében és értékelésében. Ez az iránymutatás konkrétan magában foglalhatja a nemzeti és ágazati kockázatértékeléseket, valamint az adott típusú szervezetre vonatkozó kockázatértékeléseket. Az iránymutatás a kockázatkezelési keretrendszernek az érintett szervezetek szintjén történő kidolgozására szolgáló eszközöket vagy sablonokat is tartalmazhat. A tagállamok nemzeti joga által biztosított keretek, iránymutatások vagy egyéb mechanizmusok, valamint a vonatkozó európai és nemzetközi szabványok szintén támogathatják az érintett szervezeteket az e végrehajtási rendeletnek, valamint a vonatkozó európai és nemzetközi szabványoknak való megfelelés igazolásában. Emellett az ENISA vagy az (EU) 2022/2555 irányelv szerinti illetékes nemzeti hatóságok támogathatják az érintett szervezeteket az említett kockázatértékelések során azonosított kockázatok kezelésére szolgáló megfelelő megoldások azonosításában és végrehajtásában. Ez az iránymutatás nem korlátozhatja az érintett szervezetek azon kötelezettségét, hogy azonosítsák és dokumentálják a hálózati és információs rendszerek biztonságát fenyegető kockázatokat, valamint azon kötelezettségét, hogy szükségleteiknek és erőforrásaiknak megfelelően végrehajtsák az e rendelet mellékletében meghatározott kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményeit.

(8) A hálózatbiztonsági intézkedések esetében sajátos kihívásokat jelent i. a legújabb generációs, hálózati rétegbeli kommunikációs protokollokra való átállás, ii. az elektronikus levelezésre vonatkozó, nemzetközileg elfogadott és interoperábilis, modern kommunikációs szabványok bevezetése, továbbá iii. a DNS-biztonsággal, valamint az internetes útvonal-meghatározás biztonságával és az útvonal-meghatározási higiéniával kapcsolatos bevált gyakorlatok alkalmazása tekintetben az elérhető legjobb szabványok és bevezetési technikák azonosítása. Annak érdekében, hogy az egységesen magas szintű kiberbiztonság valamennyi hálózatra kiterjedően a lehető leghamarabb biztosított legyen, a Bizottságnak az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) segítségével, valamint az illetékes hatóságokkal, az ágazattal – többek között a távközlési ágazattal – és más érdekelt felekkel együttműködve támogatnia kell egy több érdekelt felet tömörítő fórum létrehozását, amelynek feladata az említett, rendelkezésre álló legjobb szabványok és bevezetési technikák azonosítása. Az említett érdekelt felektől származó iránymutatás nem korlátozhatja az érintett szervezetek azon kötelezettségét, hogy végrehajtsák az e rendelet mellékletében meghatározott kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményeit.

(9) Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének a) pontja értelmében az alapvető és fontos szervezeteknek a kockázatelemzési szabályzatok mellett az információs rendszerek biztonságára vonatkozó szabályzatokkal is rendelkezniük kell. E célból az érintett szervezeteknek ki kell dolgozniuk a hálózati és információs rendszerek biztonságára vonatkozó szabályzatokat, valamint olyan tematikus – például hozzáférés-ellenőrzési – szabályzatokat, amelyek összhangban vannak a hálózati és információs rendszerek biztonságára vonatkozó szabályzatokkal. A hálózati és információs rendszerek biztonságára vonatkozó szabályzatnak a legmagasabb szintű dokumentumnak kell lennie, amely meghatározza az érintett szervezeteknek a hálózati és információs rendszerek biztonságára vonatkozó általános megközelítését, és azt az érintett szervezetek vezető testületeinek kell jóváhagyniuk. A témaspecifikus szabályzatokat a megfelelő vezetői szinten kell jóváhagyni. A szabályzatnak mutatókat és intézkedéseket kell meghatároznia a szabályzat végrehajtásának, valamint az érintett szervezetek hálózat- és információbiztonsága aktuális kiforrottsági szintjének nyomon követésére, különösen a kiberbiztonsági kockázatkezelési intézkedések végrehajtásának a vezető testületek általi felügyeletének megkönnyítése érdekében.

(10) Az e rendelet mellékletében meghatározott technikai és módszertani követelmények alkalmazásában a „felhasználó” kifejezés magában foglal minden olyan jogi és természetes személyt, aki vagy amely hozzáféréssel rendelkezik a szervezet hálózati és információs rendszereihez.

(11) A hálózati és információs rendszerek biztonságát fenyegető kockázatok azonosítása és kezelése érdekében az érintett szervezeteknek megfelelő kockázatkezelési keretet kell létrehozniuk és fenntartaniuk. A kockázatkezelési keret részeként az érintett szervezeteknek ki kell dolgozniuk, végre kell hajtaniuk és nyomon kell követniük egy kockázatkezelési tervet. Az érintett szervezetek a kockázatkezelési terv alapján azonosíthatják és rangsorolhatják a kockázatkezelési lehetőségeket és intézkedéseket. A kockázatkezelési lehetőségek közé tartozik különösen a kockázat elkerülése, csökkentése vagy – kivételes esetekben – elfogadása. A kockázatkezelési lehetőségek kiválasztásakor figyelembe kell venni az érintett szervezet által végzett kockázatértékelés eredményeit, és a kiválasztásnak összhangban kell lennie az érintett szervezetnek a hálózati és információs rendszerek biztonságára vonatkozó szabályzatával. A kiválasztott kockázatkezelési lehetőségek végrehajtása érdekében az érintett szervezeteknek meg kell hozniuk a megfelelő kockázatkezelési intézkedéseket.

(12) Az események, a majdnem bekövetkezett biztonsági események és a biztonsági események észlelése érdekében az érintett szervezeteknek nyomon kell követniük hálózati és információs rendszereiket, és intézkedéseket kell hozniuk az események, a majdnem bekövetkezett biztonsági események és a biztonsági események értékelésére. Ezeknek az intézkedéseknek lehetővé kell tenniük, hogy a hálózati alapú támadásokat – a rendellenes bejövő vagy kimenő adatforgalmi minták alapján –, valamint a szolgáltatásmegtagadással járó támadásokat időben észleljék.

(13) Amennyiben az érintett szervezetek üzleti hatásvizsgálatot végeznek, ajánlott, hogy olyan átfogó elemzést végezzenek, amelyben adott esetben meghatározzák a maximális elfogadható leállási időt, a helyreállítási időre vonatkozó célkitűzéseket, a helyreállítási pontra vonatkozó célkitűzéseket és a szolgáltatásnyújtási célkitűzéseket.

(14) Az érintett szervezeteknek az ellátási láncukból és beszállítóihoz fűződő kapcsolatukból eredő kockázatok csökkentése érdekében ki kell dolgozniuk az ellátási lánc védelmére vonatkozó szabályzatukat, amely szabályozza a közvetlen beszállítóikkal és szolgáltatóival fennálló kapcsolataikat. E szervezeteknek a közvetlen beszállítóikkal vagy szolgáltatókkal kötött szerződésekben megfelelő biztonsági záradékokat kell meghatározniuk, például adott esetben az (EU) 2022/2555 irányelv 21. cikkének (2) bekezdése szerinti kiberbiztonsági kockázatkezelési intézkedések meghozatalát vagy más hasonló jogi követelményeknek való megfelelést kell előírniuk.

(15) Az érintett szervezeteknek erre a célra kidolgozott szabályzat és eljárások alapján rendszeresen biztonsági teszteket kell végezniük annak ellenőrzésére, hogy a kiberbiztonsági kockázatkezelési intézkedéseket végrehajtják-e és azok megfelelően működnek-e. A biztonsági tesztek elvégezhetők adott hálózati és információs rendszereken vagy az érintett szervezet egészén, és magukban foglalhatnak automatizált vagy manuális teszteket, behatolási teszteket, sérülékenységfelmérést, statikus és dinamikus alkalmazásbiztonsági teszteket, konfigurációs teszteket vagy biztonsági ellenőrzéseket. Az érintett szervezetek biztonsági teszteket végezhetnek hálózati és információs rendszereiken azok telepítésekor, az infrastruktúra vagy az alkalmazások általuk jelentősnek ítélt korszerűsítése vagy módosítása után, illetve karbantartás után. A biztonsági tesztek eredményeinek információkkal kell szolgálniuk az érintett szervezetek számára a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére vonatkozó szabályzatok és eljárások alakításához, valamint hálózat- és információbiztonsági szabályzatok független felülvizsgálatához.

(16) A hálózati és információs rendszerek javítatlan sebezhetőségeinek kihasználása révén okozott jelentős zavarok és károk elkerülése érdekében az érintett szervezeteknek olyan megfelelő biztonsági javításkezelési eljárásokat kell meghatározniuk és alkalmazniuk, amelyek összhangban vannak az érintett szervezetek változáskezelési, sebezhetőségkezelési, kockázatkezelési és egyéb vonatkozó eljárásaival. Az érintett szervezeteknek erőforrásaikkal arányos intézkedéseket kell hozniuk annak biztosítására, hogy a biztonsági javítások ne okozzanak további sebezhetőségeket vagy instabilitásokat. Amennyiben a biztonsági javítások alkalmazása a szolgáltatás tervezett kiesésével jár, az érintett szervezeteket arra ösztönzik, hogy ügyfeleiket előzetesen megfelelően tájékoztassák.

(17) Az érintett szervezeteknek kezelniük kell az IKT-termékek vagy IKT-szolgáltatások beszállítóktól vagy szolgáltatóktól történő beszerzéséből eredő kockázatokat, és bizonyosságot kell szerezniük arról, hogy a beszerzendő IKT-termékek vagy IKT-szolgáltatások elérnek bizonyos kiberbiztonsági védelmi szinteket, például rendelkeznek az (EU) 2019/881 európai parlamenti és tanácsi rendelet ([2]) 49. cikke alapján elfogadott európai kiberbiztonsági tanúsítási rendszer keretében kibocsátott, IKT-termékekre vagy IKT-szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítvánnyal és uniós megfelelőségi nyilatkozattal. Amennyiben az érintett szervezetek a beszerzendő IKT-termékekre alkalmazandó biztonsági követelményeket határoznak meg, figyelembe kell venniük a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló európai parlamenti és tanácsi rendeletben meghatározott alapvető kiberbiztonsági követelményeket.

(18) A kiberfenyegetésekkel szembeni védelem, valamint az adatvédelmi incidensek megelőzésének és megfékezésének támogatása érdekében az érintett szervezeteknek hálózatbiztonsági megoldásokat kell alkalmazniuk. A tipikus hálózatbiztonsági megoldások közé tartoznak többek között a következők: az érintett szervezetek belső hálózatainak védelmére szolgáló tűzfalak használata; ahol feltétlenül szükség van csatlakozásra és hozzáférésre, ott a csatlakozások és a szolgáltatásokhoz való hozzáférés korlátozása; virtuális magánhálózatok használata távoli hozzáférés céljára; és a szolgáltatók általi csatlakozásnak csak engedélykérés utáni és meghatározott ideig tartó – például a karbantartási művelet időtartamára való – lehetővé tétele.

(19) Annak érdekében, hogy az érintett szervezetek megvédjék hálózataikat és információs rendszereiket a rosszindulatú és nem engedélyezett szoftverektől, olyan ellenőrzéseket kell végrehajtaniuk, amelyek megakadályozzák vagy felderítik a nem engedélyezett szoftverek használatát, továbbá adott esetben az ilyen szoftvereket észlelő és azokra reagáló szoftvereket kell használniuk. Az érintett szervezeteknek fontolóra kell venniük a támadási felület minimalizálására, a támadók által kihasználható sebezhetőségek mérséklésére, az alkalmazások végpontokon történő végrehajtásának ellenőrzésére, valamint a rosszindulatú tartalmaknak való kitettség csökkentése érdekében e-mail- és webalkalmazás-szűrők telepítésére irányuló végrehajtási intézkedések meghozatalát is.

(20) Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének g) pontja értelmében a tagállamoknak biztosítaniuk kell, hogy az alapvető és fontos szervezetek alkalmazzák az alapvető kiberhigiéniai gyakorlatokat és kiberbiztonsági képzést nyújtsanak. Az alapvető kiberhigiéniai gyakorlatok közé tartoznak többek között a következők: a zéró bizalom elve, a szoftverfrissítések, az eszközök megfelelő konfigurálása, a hálózati szegmentáció, a személyazonosság- és hozzáférés-kezelés, illetve a felhasználói tudatosság, valamint a személyzet képzése és a kiberfenyegetésekkel, az adathalászattal vagy a pszichológiai manipulációval kapcsolatos tudatosság növelése. A kiberhigiéniai gyakorlatok alkalmazása az e rendelet mellékletében meghatározott kiberbiztonsági kockázatkezelési intézkedések különböző technikai és módszertani követelményeinek részét képezik. A felhasználókra vonatkozó alapvető kiberhigiéniai gyakorlatok tekintetében az érintett szervezeteknek olyan gyakorlatokat kell figyelembe venniük, mint az íróasztal és képernyő áttekinthetőségére vonatkozó szabály, a többfaktoros és egyéb hitelesítési eszközök használata, a biztonságos e-mail-használat és webböngészés, az adathalászattal és a pszichológiai manipulációval szembeni védelem, valamint a távmunka biztonságossá tételére vonatkozó gyakorlatok.

(21) Az érintett szervezetek eszközeihez való jogosulatlan hozzáférés megakadályozása érdekében az érintett szervezeteknek témaspecifikus szabályzatot kell kidolgozniuk és alkalmazniuk, amely a személyek, valamint a hálózati és információs rendszerek, például az alkalmazások általi hozzáférésre is kiterjed.

(22) Annak elkerülése érdekében, hogy a munkavállalók sérelem- vagy károkozás céljából visszaélhessenek például az érintett szervezeten belüli hozzáférési jogokkal, az érintett szervezeteknek mérlegelniük kell a munkavállalókra vonatkozó, megfelelő biztonsági intézkedések meghozatalát, és fel kell hívniuk a személyzet figyelmét az ilyen kockázatokra. Az érintett szervezeteknek fegyelmi eljárást kell létrehozniuk, közzé tenniük és fenntartaniuk a hálózati és információs rendszerükre vonatkozó biztonsági szabályzat megsértésének kezelésére, amely eljárás beágyazható az adott érintett szervezet által létrehozott egyéb fegyelmi eljárásokba. Az érintett szervezetek alkalmazottai és adott esetben közvetlen beszállítói és szolgáltatói tekintetében elvégzett háttérellenőrzéseknek hozzá kell járulniuk az érintett szervezetek humánerőforrás-biztonsági célkitűzéséhez, és magukban foglalhatnak olyan intézkedéseket, mint például a személy bűnügyi előéletének vagy múltbeli szakmai feladatkörének – a személy érintett szervezeten belüli feladatainak megfelelően és az érintett szervezet hálózat- és információbiztonsági szabályzatával összhangban történő – ellenőrzése.

([2]) Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o., ELI: http://data.europa.eu/eli/reg/2019/2152/oj).

(23) A többfaktoros hitelesítés javíthatja a szervezetek kiberbiztonságát, és annak alkalmazását a szervezeteknek különösen akkor kell mérlegelnie, ha a felhasználók távoli helyekről férnek hozzá hálózati és információs rendszerekhez, vagy amikor érzékeny információkhoz vagy különleges jogosultságú vagy rendszeradminisztrátori felhasználói fiókokhoz férnek hozzá. A többfaktoros hitelesítés más technikákkal is kombinálható, melyek meghatározott körülmények között, előre meghatározott szabályok és minták alapján – például szokatlan helyről, szokatlan eszközről vagy szokatlan időben történő hozzáférés esetén – további faktorok alkalmazását követelik meg.

(24) Az érintett szervezeteknek megbízható eszközkezelési gyakorlatok alkalmazásával kell kezelniük és védeniük a számukra értékes eszközöket, mely eszközkezelési gyakorlatok a kockázatelemzés és az üzletmenetfolytonosság-menedzsment alapjául is kell szolgálniuk. Az érintett szervezeteknek mind a tárgyi eszközöket, mind az immateriális javakat kezelniük kell, eszközleltárt kell létrehozniuk, az eszközöket meghatározott besorolási szinthez kell társítaniuk, kezelniük kell és nyomon kell követniük az eszközöket, továbbá lépéseket kell tenniük az eszközök teljes életciklusuk alatti védelme érdekében.

(25) Az eszközkezelésnek magában kell foglalnia az eszközök típusuk, érzékenységük, kockázati szintjük és biztonsági követelményeik szerinti besorolását, valamint megfelelő intézkedések és ellenőrzések alkalmazását az eszközök rendelkezésre állásának, integritásának, bizalmas jellegének és hitelességének biztosítására. Az eszközök kockázati szint szerinti besorolása lehetővé kell tegye az érintett szervezetek számára, hogy olyan, megfelelő biztonsági intézkedéseket és ellenőrzéseket alkalmazzanak az eszközök védelme érdekében, mint a titkosítás, a hozzáférés – többek között a külső határok, illetőleg a fizikai és logikai hozzáférés – ellenőrzése, a biztonsági másolatok készítése, a naplózás és a nyomon követés, valamint a megőrzés és a megsemmisítés. Az üzleti hatásvizsgálat elvégzésekor az érintett szervezetek az eszközök zavarának a szervezetre gyakorolt következményei alapján határozhatják meg az adott eszköz besorolási szintjét. A szervezet valamennyi, eszközöket kezelő alkalmazottjának ismernie kell az eszközkezelési szabályzatokat és utasításokat.

(26) Az eszközleltár részletességének az érintett szervezetek igényeihez kell igazodnia. Egy átfogó eszközleltár a következő adatokat tartalmazhatja eszközönként: legalább egy egyedi azonosító, az eszköz tulajdonosa, az eszköz leírása, az eszköz helye, az eszköz típusa, az eszközzel kezelt információk típusa és besorolása, az eszköz legutóbbi szoftverfrissítésének időpontja vagy a legutóbbi hibajavító csomag telepítésének időpontja, az eszköz kockázatértékelés szerinti besorolása, valamint az eszköz élettartamának vége. Az eszköz tulajdonosának meghatározásakor az érintett szervezeteknek az adott eszköz védelméért felelős személyt is meg kell határoznia.

(27) A kiberbiztonsági szerepköröket, felelősségi köröket és hatásköröket úgy kell kiosztani és megszervezni, hogy olyan következetes struktúra jöjjön létre, amely lehetővé teszi a kiberbiztonság irányítását és végrehajtását az érintett szervezeteken belül, valamint biztosított legyen a hatékony kommunikáció biztonsági események esetén. Az egyes szerepkörökhöz kapcsolódó feladatok meghatározásakor és kijelölésekor az érintett szervezetek többek között az olyan szerepekörök feladatait kell mérlegelniük, mint az információbiztonsági vezető, az információbiztonsági tisztviselő, a biztonsági események kezelésével foglalkozó tisztviselő, az ellenőr vagy ezekhez hasonló szerepkörök. Az érintett szervezetek külső felekre, például harmadik fél IKT-szolgáltatókra ruházhatnak szerepköröket és feladatokat.

(28) Az (EU) 2022/2555 irányelv 21. cikkének (2) bekezdése értelmében a kiberbiztonsági kockázatkezelési intézkedéseknek minden veszélyre kiterjedő megközelítésen kell alapulniuk, amelynek célja a hálózati és információs rendszereknek és azok fizikai környezetének a védelme minden olyan esemény ellen, mint például a lopás, a tűz, az árvíz, a távközlési és áramellátási zavarok, vagy valamely alapvető vagy fontos szervezet információs és információfeldolgozó létesítményeihez való jogosulatlan fizikai hozzáférés ellen, valamint az azokban keletkezett kár és az azokon végrehajtott beavatkozás ellen, amely veszélyeztetheti a tárolt, továbbított vagy kezelt adatok vagy a hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, integritását vagy bizalmas jellegét. A kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményeinek ezért a hálózati és információs rendszerek fizikai és környezeti biztonságával is foglalkozniuk kell olyan intézkedések révén, amelyek megvédik az említett rendszereket a rendszerhibáktól, az emberi hibától, a rosszindulatú cselekményektől vagy a természeti jelenségektől. További példák a fizikai és környezeti fenyegetésekre a földrengések, a robbanások, a szabotázs, a belső fenyegetés, a polgári zavargások, a mérgező hulladékok és a környezeti kibocsátások. A hálózati és információs rendszerek elvesztésének, károsodásának vagy megfertőződésének, illetve a rendszerek működésében az őket ellátó közművek meghibásodása vagy zavara miatt bekövetkező kiesésnek a megelőzése az érintett szervezetek üzletmenet-folytonossági célkitűzéseinek részét kell képezze. Emellett a fizikai és környezeti fenyegetésekkel szembeni védelemnek hozzá kell járulnia a hálózati és információs rendszerek karbantartás alatti biztonságához az érintett szervezeteknél.

(29) Az érintett szervezeteknek védelmi intézkedéseket kell kidolgozniuk és végrehajtaniuk a fizikai és környezeti fenyegetésekkel szemben, meg kell határozniuk a fizikai és környezeti fenyegetésekre vonatkozó minimális és maximális ellenőrzési küszöbértékeket, valamint nyomon kell követniük a környezeti paramétereket. Fontolóra kell venniük például olyan rendszerek telepítését, amelyek időben észlelik azon területek víz alá kerülését, ahol a hálózati és információs rendszerek találhatók. Ami a tűzveszélyt illeti, az érintett szervezeteknek mérlegelniük kell egy külön tűzszakasz kialakítását az adatközpont védelmére, tűzálló anyagok használatát, a hőmérséklet és a páratartalom nyomon követésére szolgáló érzékelők alkalmazását, az épületnek egy olyan tűzjelző rendszerrel való összekapcsolását, amely képes automatikus értesíteni a helyi tűzoltóságot, valamint gyors reagálású tűzérzékelő és -oltó rendszerek telepítését. Emellett az érintett szervezeteknek rendszeresen tűzvédelmi gyakorlatokat és ellenőrzéseket kell végezniük. Az áramellátás biztosításával kapcsolatosan az érintett szervezeteknek számolniuk kell a vonatkozó szabványoknak megfelelő túlfeszültség elleni védelem és vészhelyzeti áramellátás telepítésének lehetőségével is. Továbbá, mivel a túlmelegedés kockázatot jelent a hálózati és információs rendszerek rendelkezésre állására nézve, az érintett szervezetek, különösen az adatközpont-szolgáltatók mérlegelhetik a megfelelő, folyamatos és redundáns légkondicionáló rendszerek használatát.

(30) E rendeletnek tovább kell pontosítania azokat az eseteket, amikor egy biztonsági eseményt az (EU) 2022/2555 irányelv 23. cikke (3) bekezdésének alkalmazásában jelentősnek kell tekinteni. A kritériumokat úgy kell meghatározni, hogy – a biztonsági eseményeknek az (EU) 2022/2555 irányelvvel összhangban történő bejelentése céljából – az érintett szervezetek számára lehetővé tegye annak értékelését, hogy egy biztonsági esemény jelentősnek minősül-e. Ezenkívül – az (EU) 2022/2555 irányelv 5. cikkének sérelme nélkül – az e rendeletben meghatározott kritériumokat kimerítőnek kell tekinteni. Ez a rendelet horizontális, illetve szervezettípusú egyedi eseteket meghatározásra révén megállapítja azokat az eseteket, amikor egy biztonsági eseményt jelentősnek kell tekinteni.

(31) Az (EU) 2022/2555 irányelv 23. cikkének (4) bekezdése értelmében az érintett szervezetek számára elő kell írni, hogy az említett rendelkezésben meghatározott határidőkön belül jelentsék be a jelentős biztonsági eseményeket. A bejelentésre vonatkozó, említett határidők attól a pillanattól számítandók, amikor a szervezet tudomást szerez a szóban forgó jelentős biztonsági eseményekről. Az érintett szervezetnek ezért be kell jelentenie azokat a biztonsági eseményeket, amelyek az első értékelés alapján súlyos működési zavart vagy pénzügyi veszteséget okozhatnak a szervezet számára, vagy jelentős vagyoni vagy nem vagyoni kárt okozásával más természetes vagy jogi személyt érinthet. Ezért ha az érintett szervezet gyanús eseményt észlelt, vagy azt követően, hogy egy harmadik fél – például magánszemély, ügyfél, szervezet, hatóság, médiaszervezet vagy más forrás – potenciális biztonsági eseményt hozott a tudomására, az érintett szervezetnek kellő időben értékelnie kell a gyanús eseményt annak megállapítása érdekében, hogy az biztonsági eseménynek minősül-e, és ha igen, meg kell határoznia annak jellegét és súlyosságát. Ezért ha az első értékelést követően az érintett szervezet kellő bizonyossággal rendelkezik arról, hogy jelentős biztonsági esemény történt, úgy kell tekinteni, hogy az érintett szervezet „tudomást szerzett” a jelentős biztonsági eseményről.

(32) Annak megállapítása érdekében, hogy egy biztonsági esemény jelentős-e, az érintett szervezeteknek adott esetben meg kell határozniuk a biztonsági esemény által érintett felhasználók számát, figyelembe véve azokat az üzleti és végfelhasználókat, akikkel az érintett szervezet szerződéses viszonyban van, valamint az üzleti ügyfelekkel kapcsolatban álló természetes és jogi személyeket. Amennyiben az érintett szervezet nem tudja kiszámítani az érintett felhasználók számát, a biztonsági esemény által érintett felhasználók teljes számának kiszámításához az érintett szervezetnek az érintett felhasználók lehetséges maximális számára vonatkozó becslését kell figyelembe venni. A bizalmi szolgáltatásokat érintő biztonsági események jelentőségének megállapításához nemcsak a felhasználók, hanem az igénybe vevő felek számát is meg kell határozni, mivel a bizalmi szolgáltatásokat érintő jelentős biztonsági események által okozott működési zavarok és a vagyoni vagy nem vagyoni károk őket is ugyanúgy érinthetik. Ezért a bizalmi szolgáltatóknak adott esetben az igénybe vevő felek számát is figyelembe kell venniük annak megállapításakor, hogy egy biztonsági esemény jelentős-e. E célból igénybe vevő feleken olyan természetes vagy jogi személyeket kell érteni, akik vagy amelyek igénybe veszik az adott bizalmi szolgáltatást.

(33) Azok a karbantartási műveletek, amelyek a szolgáltatások korlátozott rendelkezésre állásával vagy rendelkezésre állásának szünetelésével járnak, nem tekintendők jelentős biztonsági eseménynek, ha a szolgáltatás korlátozott rendelkezésre állása vagy rendelkezésre állásának szünetelése tervezett karbantartási művelet következtében történik. Továbbá nem tekinthető jelentős biztonsági eseménynek, ha egy szolgáltatás tervezett üzemszünet – például előre meghatározott szerződéses megállapodáson alapuló üzemszünet vagy a rendelkezésre állás ilyen megállapodáson alapuló szünetelése – miatt nem érhető el.

(34) A szolgáltatás rendelkezésre állását befolyásoló biztonsági esemény időtartamának az érintett szolgáltatás megfelelő nyújtásának zavarától a helyreállás időpontjáig terjedő időtartamot kell tekinteni. Amennyiben az érintett szervezet nem tudja meghatározni a zavar kezdetének időpontját, a biztonsági esemény időtartamát vagy attól az időponttól kell mérni, amikor a biztonsági eseményt észlelték, vagy pedig attól az időponttól, amikor a biztonsági eseményt a hálózati vagy rendszernaplókban vagy más adatforrásokban rögzítették, attól függően, hogy melyik időpont a korábbi.

(35) Az az időtartam, amely alatt a szolgáltatás rendelkezésre állása teljesen szünetel, attól a pillanattól kezdődik, amikor a szolgáltatás teljes mértékben elérhetetlenné válik a felhasználók számára, és addig a pillanatig tart, amikor a szokásos tevékenységek vagy műveletek visszaállnak a szolgáltatás biztonsági eseményt megelőző színvonalára. Amennyiben az érintett szervezet nem tudja meghatározni, hogy mikortól szűnt meg teljesen a szolgáltatás rendelkezésre állása, a rendelkezésre állás szünetelését attól az időponttól kell mérni, amikor azt az adott szervezet észlelte.

(36) A biztonsági eseményekből eredő közvetlen pénzügyi veszteségek meghatározása céljából az érintett szervezetnek figyelembe kell vennie az adott biztonsági esemény következtében elszenvedett valamennyi pénzügyi veszteséget, például a szoftver, hardver vagy infrastruktúra cseréjével vagy áthelyezésével kapcsolatos költségeket, a személyzeti költségeket, beleértve a személyzet leváltásával vagy áthelyezésével, a további személyzet felvételével, a túlórák díjazásával és az elveszett vagy csökkent készségek helyreállításával kapcsolatos költségeket, a szerződéses kötelezettségek be nem tartása következtében fizetendő díjakat, az ügyfeleknek nyújtott jogorvoslat és kártérítés költségeit, az elmaradt bevételekből eredő veszteségeket, a belső és külső kommunikációval kapcsolatos költségeket, a tanácsadásért fizetett költségeket, beleértve a jogi tanácsadással, az igazságügyi szakértői szolgáltatásokkal és a helyreállításra irányuló szolgáltatásokkal összefüggő költségeket, valamint a biztonsági eseményhez kapcsolódó egyéb költségeket. A közigazgatási bírságok, valamint a napi ügyvitel költségei – többek között az infrastruktúra, a berendezések, a hardver és a szoftver általános karbantartásának költségei, a személyzet készségeinek naprakészen tartásához kapcsolódó költségek, az üzleti tevékenységnek a biztonsági eseményt követő megerősítéséhez kapcsolódó belső vagy külső költségek, beleértve a fejlesztéseket, a javításokat és a kockázatértékelési kezdeményezéseket, valamint a biztosítási díjak – azonban nem tekinthetők biztonsági eseményből eredő pénzügyi veszteségnek. Az érintett szervezetnek a rendelkezésre álló adatok alapján kell kiszámítania a pénzügyi veszteségek összegét, és amennyiben a pénzügyi veszteségek tényleges összege nem határozható meg, ezeket az összegeket meg kell becsülnie.

(37) Az érintett szervezetet továbbá azon biztonsági események jelentésére is kötelezni kell, amelyek természetes személyek halálát vagy jelentős egészségkárosodását okozták vagy okozhatják, mivel az ilyen biztonsági események a jelentős vagyoni vagy nem vagyoni kár okozásának különösen súlyos eseteit képezik. Például előfordulhat, hogy az érintett szervezetnél bekövetkező biztonsági esemény hatására az egészségügyi ellátás vagy a segélyhívó szolgálatok elérhetetlenné válnak, illetve sérül bizonyos adatok bizalmas jellege vagy integritása, ami hatással lehet természetes személyek egészségére. Annak meghatározása céljából, hogy egy biztonsági esemény valamely természetes személy egészségkárosodását okozta-e vagy okozhatja-e, az érintett szervezetnek figyelembe kell vennie, hogy az adott biztonsági esemény okozott-e vagy okozhat-e súlyos sérüléseket és megbetegedést. E célból az érintett szervezet nem kötelezhető olyan további információk gyűjtésére, amelyekhez nem fér hozzá.

(38) Korlátozott rendelkezésre állásnak tekintendő különösen az az eset, amikor az érintett szervezet által nyújtott szolgáltatás válaszideje jelentősen lassabb az átlagosnál, vagy ha egy szolgáltatás nem minden funkciója áll rendelkezésre. Amennyiben lehetséges, a válaszidőben jelentkező késés értékelésére az érintett szervezet által nyújtott szolgáltatások átlagos válaszidején alapuló, objektív kritériumokat kell alkalmazni. Szolgáltatás által nyújtott funkció lehet például csevegőfunkció vagy képkeresési funkció.

(39) Az érintett szervezet hálózati és információs rendszereihez való sikeres, gyaníthatóan rosszindulatú és jogosulatlan hozzáférést jelentős biztonsági eseménynek kell tekinteni, amennyiben az ilyen hozzáférés súlyos működési zavart okozhat. Jelentős biztonsági eseménynek tekintendő például, hogy egy kiberbiztonsági fenyegetést jelentő szereplő előre hozzáférést biztosít magának az érintett szervezet hálózati és információs rendszereihez azzal a céllal, hogy a jövőben zavart okozzon a szolgáltatásokban.

(40) Azokat az ismétlődő biztonsági eseményeket, amelyek ugyanahhoz a nyilvánvaló kiváltó okhoz kapcsolódnak, de amelyek külön-külön nem minősülnének jelentős biztonsági eseménynek, együttesen jelentős biztonsági eseménynek kell tekinteni, amennyiben együttesen megfelelnek a pénzügyi veszteségre vonatkozó kritériumnak, és hat hónapon belül legalább kétszer bekövetkeztek. Az ilyen ismétlődő biztonsági események jelentős hiányosságokra és gyengeségekre utalhatnak az érintett szervezet kiberbiztonsági kockázatkezelési eljárásaiban és kiberbiztonsági kiforrottsági szintjében. Továbbá a szóban forgó ismétlődő események jelentős pénzügyi veszteséget okozhatnak az érintett szervezetnek.

(41) A Bizottság az (EU) 2022/2555 irányelv 21. cikkének (5) bekezdésével és 23. cikkének (11) bekezdésével összhangban megosztotta a szakértelmet és együttműködött az együttműködési csoporttal és az ENISA-val a végrehajtási jogi aktus tervezetével kapcsolatban.

(42) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([3]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2024. szeptember 1-jén véleményt nyilvánított.

(43) Az e rendeletben előírt intézkedések összhangban vannak az (EU) 2022/2555 irányelv 39. cikke szerint létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Tárgy

E rendelet meghatározza az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésében említett intézkedések technikai és módszertani követelményeit a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók (a továbbiakban: érintett szervezetek) tekintetében, valamint pontosítja azokat az eseteket, amelyekben egy biztonsági eseményt az (EU) 2022/2555 irányelv 23. cikke (3) bekezdésének értelmében vett jelentős biztonsági eseménynek kell tekinteni.

2. cikk

Technikai és módszertani követelmények

(1) Az érintett szervezetek tekintetében az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének a)–j) pontjában említett kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményeit e rendelet melléklete határozza meg.

(2) Az érintett szervezetek biztosítják, hogy a kiberbiztonsági kockázatkezelési intézkedésekre vonatkozó, e rendelet mellékletében meghatározott technikai és módszertani követelmények végrehajtása és alkalmazása során a hálózati és információs rendszerek biztonsági szintje arányos legyen a felmerülő kockázatokkal. E célból a kiberbiztonsági kockázatkezelési intézkedések e rendelet mellékletében meghatározott műszaki és módszertani követelményeinek való megfelelés során kellően figyelembe veszik a kitettségük mértékét, a méretüket, valamint a biztonsági események bekövetkezésének valószínűségét és súlyosságát, beleértve azok társadalmi és gazdasági hatását.

([3]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Amennyiben e rendelet melléklete úgy rendelkezik, hogy valamely kiberbiztonsági kockázatkezelési intézkedésre vonatkozó technikai vagy módszertani követelmény akkor alkalmazandó, „ha indokolt”, „ha releváns” vagy „ha megvalósítható”, de az érintett szervezet úgy ítéli meg, hogy az adott technikai vagy módszertani követelmény alkalmazása nem indokolt, nem releváns vagy nem megvalósítható, az érintett szervezetnek érthető módon dokumentálnia kell az erre vonatkozó érvelését.

3. cikk

Jelentős biztonsági események

(1) Egy biztonsági esemény az (EU) 2022/2555 irányelv 23. cikke (3) bekezdésének alkalmazásában akkor tekintendő jelentősnek az érintett szervezetek tekintetében, ha az alábbi kritériumok közül legalább egy teljesül:

a) a biztonsági esemény az érintett szervezetnek 500 000 EUR-t vagy az előző pénzügyi évben elért teljes éves árbevételének 5 %-át (amelyik alacsonyabb) meghaladó közvetlen pénzügyi veszteséget okozott vagy okozhat;

b) a biztonsági esemény az érintett szervezet (EU) 2016/943 irányelv 2. cikkének 1. pontja szerinti üzleti titkainak kiszivárgását okozta vagy okozhatja;

c) a biztonsági esemény valamely természetes személy halálát okozta vagy okozhatja;

d) a biztonsági esemény valamely természetes személy egészségkárosodását okozta vagy okozhatja;

e) a hálózati és információs rendszerekhez olyan sikeres, gyaníthatóan rosszindulatú és jogosulatlan hozzáférés történt, amely súlyos működési zavarokat okozhat;

f) a biztonsági esemény megfelel a 4. cikkben meghatározott kritériumoknak;

g) a biztonsági esemény megfelel egy vagy több, az 5–14. cikkben meghatározott kritériumnak.

(2) Az érintett szervezetek által vagy nevében végzett tervezett karbantartási műveletek miatti tervezett üzemszünetek, illetve az említett karbantartási műveletek tervezett következményei nem tekintendők jelentős biztonsági eseménynek.

(3) Az esemény által érintett felhasználók számának a 7. és 9–14. cikk alkalmazásában történő kiszámításakor az érintett szervezetnek figyelembe kell vennie az alábbiak mindegyikét:

a) azon ügyfelek száma, akik olyan szerződést kötöttek az érintett szervezettel, amely hozzáférést biztosít számukra az érintett szervezet hálózati és információs rendszereihez vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül hozzáférhető szolgáltatásokhoz;

b) az üzleti ügyfelekkel kapcsolatban álló olyan természetes és jogi személyek száma, akik az érintett szervezet hálózati és információs rendszereit vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül hozzáférhető szolgáltatásokat használják.

4. cikk

Ismétlődő események

Azokat a biztonsági eseményeket, amelyek önmagukban nem minősülnek a 3. cikk értelmében vett jelentős biztonsági eseménynek, együttesen egyetlen jelentős biztonsági eseménynek kell tekinteni, amennyiben megfelelnek az alábbi kritériumok mindegyikének:

a) 6 hónapon belül legalább kétszer előfordultak;

b) ugyanahhoz a nyilvánvaló kiváltó okhoz kapcsolódnak;

c) együttesen megfelelnek a 3. cikk (1) bekezdésének a) pontjában meghatározott kritériumoknak.

5. cikk

A DNS-szolgáltatók tekintetében jelentősnek minősülő biztonsági események

A DNS-szolgáltatók tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) a rekurzív vagy autoritatív doménnévfeloldási szolgáltatás több mint 30 percig egyáltalán nem áll rendelkezésre;

b) a rekurzív vagy autoritatív doménnévfeloldási szolgáltatás DNS-kérelmekre adott válaszainak átlagos válaszideje egy óránál hosszabb ideig meghaladja a 10 másodpercet;

c) az autoritatív doménnévfeloldási szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége sérült, kivéve azokat az eseteket, amikor a DNS-szolgáltató által kezelt doménnevek legfeljebb 1 %-át képviselő, kevesebb mint 1 000 doménnév adatai pontatlanok hibás konfiguráció miatt.

6. cikk

A legfelső szintű doménnév-nyilvántartók tekintetében jelentősnek minősülő biztonsági események

A legfelső szintű doménnév-nyilvántartók tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) az autoritatív doménnévfeloldási szolgáltatás egyáltalán nem áll rendelkezésre;

b) az autoritatív doménnévfeloldási szolgáltatás DNS-kérelmekre adott válaszainak átlagos válaszideje egy óránál hosszabb ideig meghaladja a 10 másodpercet;

c) a legfelső szintű doménnév-nyilvántartó technikai működésével összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége sérül.

7. cikk

A felhőszolgáltatók tekintetében jelentősnek minősülő biztonsági események

A felhőszolgáltatók tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) a nyújtott felhőszolgáltatás több mint 30 percig egyáltalán nem áll rendelkezésre;

b) a szolgáltató felhőszolgáltatása a felhőszolgáltatást igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, a felhőszolgáltatást igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egy óránál hosszabb ideig korlátozottan áll rendelkezésre;

c) a felhőszolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

d) a felhőszolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott felhőszolgáltatást igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott felhőszolgáltatást igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

8. cikk

Az adatközpontok tekintetében jelentősnek minősülő biztonsági események

Az adatközpontok tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) a szolgáltató által üzemeltetett adatközpont adatközpont-szolgáltatása egyáltalán nem áll rendelkezésre;

b) a szolgáltató által üzemeltetett adatközpont adatközpont-szolgáltatása több mint egy órán át csak korlátozottan áll rendelkezésre;

c) az adatközpont-szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

d) a szolgáltató által működtetett adatközponthoz való fizikai hozzáféréssel kapcsolatban problémák merültek fel.

9. cikk

A tartalomszolgáltató hálózati szolgáltatók tekintetében jelentősnek minősülő biztonsági események

A tartalomszolgáltató hálózati szolgáltatók tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) a tartalomszolgáltató hálózat több mint 30 percig egyáltalán nem áll rendelkezésre;

b) a tartalomszolgáltató hálózat a tartalomszolgáltató hálózatot igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, a tartalomszolgáltató hálózatot igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egy óránál hosszabb ideig korlátozottan áll rendelkezésre;

c) a tartalomszolgáltató hálózat rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

d) a tartalomszolgáltató hálózat rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott tartalomszolgáltató hálózatot igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott tartalomszolgáltató hálózatot igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

10. cikk

Az irányított szolgáltatók és az irányított biztonsági szolgáltatók tekintetében jelentősnek minősülő biztonsági események

Az irányított szolgáltatók és az irányított biztonsági szolgáltatók tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) az irányított szolgáltatás vagy az irányított biztonsági szolgáltatás több mint 30 percig egyáltalán nem áll rendelkezésre;

b) az irányított szolgáltatás vagy az irányított biztonsági szolgáltatás a szolgáltatást igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, a szolgáltatást igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egy óránál hosszabb ideig korlátozottan áll rendelkezésre;

c) az irányított szolgáltatás vagy az irányított biztonsági szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

d) az irányított szolgáltatás vagy az irányított biztonsági szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott irányított szolgáltatást vagy az adott irányított biztonsági szolgáltatást igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott irányított szolgáltatást vagy az adott irányított biztonsági szolgáltatást igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

11. cikk

Az online piacterek szolgáltatói tekintetében jelentősnek minősülő biztonsági események

Az online piacterek szolgáltatói tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) az online piactér az azt igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, az online piacteret igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egyáltalán nem érhető el;

b) az online piactér korlátozott rendelkezésre állása az azt igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy a korlátozott rendelkezésre állás több mint 1 millió, az adott online piacteret igénybe vevő uniós felhasználót érint (amelyik szám kisebb);

c) az online piactér rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

d) az online piactér rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott online piacteret igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott online piacteret igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

12. cikk

Az online keresőprogramok szolgáltatói tekintetében jelentősnek minősülő biztonsági események

Az online keresőprogramok szolgáltatói tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) az online keresőprogram az azt igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, az adott online keresőprogramot igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egyáltalán nem érhető el;

b) az online keresőprogram korlátozott rendelkezésre állása az azt igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy a korlátozott rendelkezésre állás több mint 1 millió, az adott online keresőprogramot igénybe vevő uniós felhasználót érint (amelyik szám kisebb);

c) az online keresőprogram rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

d) az online keresőprogram rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott online keresőprogramot igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott online keresőprogramot igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

13. cikk

A közösségimédia-szolgáltatási platformok szolgáltatói tekintetében jelentősnek minősülő biztonsági események

A közösségimédia-szolgáltatási platformok szolgáltatói tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) a közösségimédia-szolgáltatási platform az azt igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, az adott közösségimédia-szolgáltatási platformot igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egyáltalán nem érhető el;

b) a közösségimédia-szolgáltatási platform korlátozott rendelkezésre állása az azt igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy a korlátozott rendelkezésre állás több mint 1 millió, az adott közösségimédia-szolgáltatási platformot igénybe vevő uniós felhasználót érint (amelyik szám kisebb);

c) a közösségimédia-szolgáltatási platform rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

d) a közösségimédia-szolgáltatási platform rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott közösségimédia-szolgáltatási platformot igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott közösségimédia-szolgáltatási platformot igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

14. cikk

A bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események

A bizalmi szolgáltatók tekintetében egy biztonsági esemény akkor minősül a 3. cikk (1) bekezdésének g) pontja értelmében jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) a bizalmi szolgáltatás több mint 20 percig egyáltalán nem áll rendelkezésre;

b) a bizalmi szolgáltatás naptári hetek alapján számítva egy óránál hosszabb ideig nem érhető el a felhasználók vagy az igénybe vevő felek számára;

c) a bizalmi szolgáltatás korlátozott rendelkezésre állása a szolgalátatás uniós felhasználóinak vagy uniós igénybe vevő feleinek több mint 1 %-át, vagy több mint 200 000 uniós felhasználóját vagy igénybe vevő uniós felét érinti (amelyik szám kisebb);

d) fizikai hozzáférés történt egy olyan területhez, ahol hálózati és információs rendszerek találhatók, és amelyhez a hozzáférés csak a bizalmi szolgáltató megbízható személyzete számára engedélyezett, vagy az ilyen területhez való fizikai hozzáférés védelme sérült;

e) a bizalmi szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely a bizalmi szolgáltatás uniós felhasználólóinak vagy uniós igénybe vevő feleinek több mint 0,1 %-át, vagy több mint 100 uniós felhasználóját vagy igénybe vevő felét érinti (amelyik szám kisebb).

15. cikk

Hatályon kívül helyezés

Az (EU) 2018/151 bizottsági végrehajtási rendelet ([4]) hatályát veszti.

16. cikk

Hatálybalépés és alkalmazás

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2024. október 17-én.

a Bizottság részéről
Ursula VON DER LEYEN
az elnök

([4]) A Bizottság (EU) 2018/151 végrehajtási rendelete (2018. január 30.) a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról (HL L 26., 2018.1.31., 48. o., ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

MELLÉKLET

Az e rendelet 2. cikkében említett technikai és módszertani követelmények

1. **A hálózati és informatikai rendszerek biztonságára vonatkozó szabályzat (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének a) pontja)**

1.1. *A hálózati és informatikai rendszerek biztonságára vonatkozó szabályzat*

1.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése a) pontjának alkalmazásában a hálózati és informatikai rendszerek biztonságára vonatkozó szabályzat:

a) meghatározza az érintett szervezetek hálózati és informatikai rendszereik biztonságának kezelésére vonatkozó megközelítését;

b) megfelel az érintett szervezetek üzleti stratégiájának és célkitűzéseinek, és kiegészíti azokat;

c) meghatározza a hálózati és informatikai biztonságra vonatkozó célkitűzéseket;

d) a hálózati és informatikai rendszerek biztonságának folyamatos javítására irányuló kötelezettségvállalást tartalmaz;

e) a végrehajtáshoz szükséges megfelelő források – ezen belül a szükséges személyzet, pénzügyi erőforrások, folyamatok, eszközök és technológiák – biztosítására vonatkozó kötelezettségvállalást tartalmaz;

f) ismertetésre kerül az érintett alkalmazottak és az érintett külső érdekelt felek számára, akik tudomásul veszik az abban foglaltakat;

g) meghatározza az 1.2. pont szerinti szerepköröket és felelősségi köröket;

h) felsorolja a megőrzendő dokumentumokat, és azt, hogy az egyes dokumentumokat meddig kell megőrizni;

i) felsorolja a témaspecifikus szabályzatokat;

j) meghatározza a végrehajtás nyomon követésére szolgáló mutatókat és intézkedéseket, valamint az érintett szervezetek hálózat- és információbiztonsággal kapcsolatos fejlettségi szintjének jelenlegi állapotát;

k) feltünteti az érintett szervezetek vezető testületei (a továbbiakban: vezető testületek) általi hivatalos jóváhagyás időpontját.

1.1.2. A vezető testületek évente legalább egyszer, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a hálózati és információs rendszerek biztonságára vonatkozó szabályzatot. A felülvizsgálatok eredményét dokumentálni kell.

1.2. *Szerepkörök, felelősségi körök és hatáskörök*

1.2.1. A hálózati és információs rendszereik biztonságára vonatkozó, 1.1. pontban említett szabályzat részeként az érintett szervezet meghatározza a hálózati és információs rendszerek biztonságával kapcsolatos felelősségi köröket és hatásköröket, azokat az adott szervezet igényeinek megfelelően kiosztva különböző szerepekhez rendeli, és erről tájékoztatja a vezető testületeket.

1.2.2. Az érintett szervezet előírja valamennyi alkalmazottja és a harmadik felek számára, hogy az érintett szervezet hálózat- és információbiztonsági szabályzatával, tematikus szabályzataival és eljárásaival összhangban biztosítsák a hálózati és információs rendszerek biztonságát.

1.2.3. Legalább egy személy közvetlenül a vezető testületnek tesz jelentést a hálózati és információs rendszerek biztonságával kapcsolatos kérdésekről.

1.2.4. Az érintett szervezet méretétől függően a hálózati és információs rendszerek biztonsága külön szerepkör, vagy a meglévő szerepkörökhöz rendelt új kötelezettségek kijelölését igényli.

1.2.5. Ha releváns, az egymásnak ellentmondó feladatokat és az összeférhetetlen hatásköröket el kell különíteni.

1.2.6. A vezető testületek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a szerepeket, felelősségi köröket és hatásköröket.

2. **Kockázatkezelési szabályzat (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének a) pontja)**

2.1. *Kockázatkezelési keret*

2.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése a) pontjának alkalmazásában az érintett szervezetek megfelelő kockázatkezelési keretet hoznak létre és tartanak fenn a hálózati és információs rendszerek biztonságát fenyegető kockázatok azonosítása és kezelése érdekében. Az érintett szervezetek kockázatértékeléseket végeznek, azokat dokumentálják, és az eredmények alapján kockázatkezelési tervet dolgoznak ki, hajtanak végre és követnek. A kockázatértékelés eredményeit és a fennmaradó kockázatokat a vezető testületek, vagy ha releváns, az elszámoltatható és kockázatkezelési jogosultsággal rendelkező személyek fogadják el, feltéve, hogy az érintett szervezetek biztosítják a megfelelő jelentéstételt a vezető testületek felé.

2.1.2. A 2.1.1. pont alkalmazásában az érintett szervezetek eljárásokat dolgoznak ki a kockázatok azonosítására, elemzésére, értékelésére és kezelésére („kiberbiztonsági kockázatkezelési eljárás”). A kiberbiztonsági kockázatkezelési eljárás, ha releváns, az érintett szervezetek általános kockázatkezelési eljárásának szerves részét képezi. A kiberbiztonsági kockázatkezelési eljárás keretében az érintett szervezetek:

a) kockázatkezelési módszertant követnek;

b) az érintett szervezet kockázatvállalási hajlandóságának megfelelően megállapítják a kockázati toleranciaszintet;

c) megfelelő kockázati kritériumokat határoznak meg és tartanak fenn;

d) az összes veszélyre kiterjedő megközelítéssel összhangban azonosítják és dokumentálják a hálózati és információs rendszerek biztonságát érintő kockázatokat, különösen a harmadik felekkel kapcsolatban, valamint azokat a kockázatokat, amelyek zavarokat okozhatnak a hálózati és információs rendszerek rendelkezésre állásában, integritásában, hitelességében és bizalmas jellegében, beleértve az egyetlen ponton bekövetkező meghibásodás azonosítását is;

e) elemzik a hálózati és információs rendszerek biztonságát fenyegető kockázatokat, ezen belül a fenyegetés jellegét, a bekövetkezés valószínűségét, a kockázatok hatását és a kockázati szintet, figyelembe véve a kiberfenyegetésekkel kapcsolatos hírszerzést és a sebezhetőségeket;

f) a kockázati kritériumok alapján elvégzik az azonosított kockázatok értékelését;

g) azonosítják és rangsorolják a megfelelő kockázatkezelési lehetőségeket és intézkedéseket;

h) folyamatosan nyomon követik a kockázatkezelési intézkedések végrehajtását;

i) meghatározzák, hogy ki felelős a kockázatkezelési intézkedések végrehajtásáért, és hogy mikor kell azokat végrehajtani;

j) a kockázatkezelési tervben átfogó módon dokumentálják a kiválasztott kockázatkezelési intézkedéseket és a fennmaradó kockázatok elfogadását alátámasztó okokat.

2.1.3. A megfelelő kockázatkezelési lehetőségek és intézkedések azonosítása és rangsorolása során az érintett szervezetek figyelembe veszik a kockázatértékelés eredményeit, a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére szolgáló eljárás eredményeit, a végrehajtás költségeit a várható előnyök fényében, a 12.1. pontban említett eszközminősítést és a 4.1.3. pontban említett üzleti hatásvizsgálatot.

2.1.4. Az érintett szervezetek tervezett időközönként, legalább évente, illetve a működést érintő nagyobb változások, kockázatok felmerülése vagy jelentős biztonsági esemény bekövetkezése esetén felülvizsgálják, és ha indokolt, frissítik a kockázatértékelés eredményeit és a kockázatkezelési tervet.

2.2. *A megfelelőség ellenőrzése*

2.2.1. Az érintett szervezetek rendszeresen felülvizsgálják a hálózati és információs rendszerek biztonságára vonatkozó szabályzatuknak, a tematikus szabályzataiknak, a szabályoknak és szabványoknak való megfelelést. A megfelelőségi felülvizsgálatok alapján a vezető testületeket rendszeres jelentések útján tájékoztatni kell a hálózat- és információbiztonság állapotáról.

2.2.2. Az érintett szervezetek szervezeti felépítésüknek, működési környezetüknek és fenyegetettségi helyzetüknek megfelelő, hatékony megfelelési jelentéstételi rendszert vezetnek be. A megfelelési jelentéstételi rendszert úgy kell kialakítani, hogy az alapján a vezető testületek megalapozott véleményt alakíthassanak ki az érintett szervezet kockázatkezelésének aktuális helyzetéről.

2.2.3. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén ellenőrzik a megfelelőséget.

2.3. *Az információ- és hálózatbiztonság független felülvizsgálata*

2.3.1. Az érintett szervezetek független módon felülvizsgálják a hálózati és információs rendszerek biztonságának kezelésére vonatkozó megközelítésüket és annak végrehajtását, beleértve az embereket, a folyamatokat és a technológiákat is.

2.3.2. Az érintett szervezetek eljárásokat dolgoznak ki és tartanak fenn a független felülvizsgálatok elvégzésére, amelyeket az ellenőrzés terén megfelelő szakértelemmel rendelkező személyek végeznek el. Amennyiben a független felülvizsgálatot az érintett szervezet személyzetének tagjai végzik, a felülvizsgálatot végző személyek nem lehetnek a felülvizsgálat tárgyát képező területtel foglalkozó illetékes személyzet tagjai. Ha az érintett szervezet mérete nem teszi lehetővé a hatáskörök ilyen szétválasztását, az érintett szervezet alternatív intézkedéseket vezet be a felülvizsgálatok pártatlanságának biztosítása érdekében.

2.3.3. A független felülvizsgálatok eredményeit, beleértve a 2.2. pont szerinti megfelelőség-ellenőrzés, valamint a 7. pont szerinti nyomon követés és mérés eredményeit is, jelenteni kell a vezető testületek felé. Az érintett szervezet kockázat-jóváhagyási kritériumaival összhangban korrekciós intézkedéseket kell hozni vagy a fennmaradó kockázatokat el kell fogadni.

2.3.4. A független felülvizsgálatokat tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén kell elvégezni.

3. **Biztonsági esemény kezelése (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének b) pontja)**

3.1. *A biztonsági események kezelésére vonatkozó szabályzat*

3.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése b) pontjának alkalmazásában az érintett szervezet a biztonsági események kezelésére vonatkozó szabályzatot dolgoz ki és hajt végre, amely meghatározza a biztonsági események kellő időben történő észlelésére, elemzésére, enyhítésére vagy az azokra való reagálásra, valamint az említett események utáni helyreállításra, dokumentálásra és jelentéstételre vonatkozó szerepköröket, felelősségi köröket és eljárásokat.

3.1.2. A 3.1.1. pontban említett szabályzatot a 4.1. pontban említett üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervvel összhangban kell kidolgozni. A szabályzat a következőket tartalmazza:

a) a biztonsági események olyan kategorizálási rendszere, amely összhangban áll a 3.4.1. pont szerint elvégzett eseményértékeléssel és -besorolással;

b) hatékony – az eszkalációra és a bejelentésre is érvényes – kommunikációs tervek;

c) a biztonsági események észlelésére és az azokra való megfelelő reagálásra szolgáló szerepek illetékes alkalmazottak közötti kiosztása;

d) a biztonsági események észlelése és az azokra való reagálás során használandó dokumentumok, például eseménykezelési kézikönyvek, eszkalációs ábrák, kontaktszemélyek listája és sablonok.

3.1.3. A szabályzatban meghatározott szerepeket, felelősségi köröket és eljárásokat tervezett időközönként, illetve jelentős biztonsági események bekövetkezése, a működést érintő nagyobb változások bevezetése vagy kockázatok felmerülése után tesztelni, értékelni, és ha indokolt, frissíteni kell.

3.2. *Nyomon követés és naplózás*

3.2.1. Az érintett szervezetek eljárásokat dolgoznak ki és eszközöket használnak a hálózati és információs rendszereiket érintő tevékenységek nyomon követésére és naplózására a biztonsági eseménynek minősülő események észlelése és a hatások enyhítését célzó megfelelő válaszlépések érdekében.

3.2.2. Ha megvalósítható, a nyomon követést automatizálni kell, és a szervezeti kapacitásnak megfelelően folyamatosan vagy rendszeres időközönként kell végezni. Az érintett szervezetek nyomonkövetési tevékenységeiket oly módon végzik, hogy a lehető legkisebbre csökkentsék a hamis pozitív és hamis negatív eredményeket.

3.2.3. A 3.2.1. pontban említett eljárások alapján az érintett szervezetek naplókat vezetnek, azokat dokumentálják és felülvizsgálják. Az érintett szervezetek a 2.1. pont szerint elvégzett kockázatértékelés eredményei alapján összeállítják a naplózandó eszközök jegyzékét. Ha indokolt, a naplók a következőket tartalmazzák:

a) releváns kimenő és bejövő hálózati forgalom;

b) az érintett szervezetek hálózati és információs rendszerei felhasználóinak létrehozása, módosítása vagy törlése, valamint az engedélyek kiterjesztése;

c) a rendszerekhez és alkalmazásokhoz való hozzáférés;

d) a hitelesítésekkel kapcsolatos események;

e) a rendszerekhez és alkalmazásokhoz való minden kiemelt hozzáférés, valamint a rendszergazda jogosultsággal rendelkező fiókokból végzett tevékenységek;

f) a kritikus konfigurációs fájlokhoz és biztonsági mentésekhez tartozó fájlokhoz való hozzáférés vagy azok módosítása;

g) eseménynaplók és biztonsági eszközökből, például vírusirtó rendszerekből, behatolásérzékelő rendszerekből vagy tűzfalakból származó naplók;

h) a rendszererőforrások használata, valamint azok teljesítménye;

i) a létesítményekhez való fizikai hozzáférés;

j) a hálózati berendezésekhez és eszközökhöz való hozzáférés és azok használata;

k) a különböző naplók aktiválása, leállítása és szüneteltetése;

l) környezeti események.

3.2.4. A nyilvántartásokat a szokatlan vagy nemkívánatos tendenciák feltárása érdekében rendszeresen ellenőrizni kell. Ha indokolt, az érintett szervezetek megfelelő riasztási küszöbértékeket állapítanak meg. A riasztási küszöbérték túllépése, ha indokolt, automatikusan aktiválja a riasztást. Az érintett szervezetek gondoskodnak arról, hogy riasztás esetén időben sor kerüljön a kompetens és megfelelő válaszintézkedés megtételére.

3.2.5. Az érintett szervezetek előre meghatározott ideig megőrzik a naplókat, azokról biztonsági mentést készítenek, és gondoskodnak arról, hogy azokhoz jogosulatlanul senki ne férjen hozzá, illetve hogy azokat jogosulatlanul senki ne módosíthassa.

3.2.6. Ha megvalósítható, az érintett szervezetek gondoskodnak arról, hogy valamennyi rendszerük szinkronizált időbeállítási forrásokkal működjön, ami lehetővé teszi a rendszernaplóknak az események értékelése céljából történő összehasonlítását. Az érintett szervezetek összeállítják és vezetik a naplózott eszközök jegyzékét, és gondoskodnak a felügyeleti és naplózási rendszerek redundanciájáról. A felügyeleti és naplózási rendszerek rendelkezésre állását az általuk felügyelt rendszerektől függetlenül kell ellenőrizni.

3.2.7. Az eljárásokat, valamint a naplózott eszközök jegyzékét rendszeres időközönként, illetve jelentős biztonsági eseményeket követően felül kell vizsgálni, és ha indokolt, frissíteni kell.

3.3. *Eseményjelentések*

3.3.1. Az érintett szervezetek egyszerű mechanizmust vezetnek be, amely lehetővé teszi alkalmazottaik, beszállítóik és ügyfeleik számára a gyanús események bejelentését.

3.3.2. Az érintett szervezetek, ha indokolt, tájékoztatják beszállítóikat és ügyfeleiket az eseményjelentési mechanizmusról, és rendszeres képzéseket tartanak alkalmazottaik számára a mechanizmus használatáról.

3.4. *A biztonsági események értékelése és minősítése*

3.4.1. Az érintett szervezetek kiértékelik a gyanús eseményeket annak megállapítása érdekében, hogy azok biztonsági eseménynek minősülnek-e, és ha igen, meghatározzák azok jellegét és súlyosságát.

3.4.2. A 3.4.1. pont alkalmazásában az érintett szervezetek a következőképpen járnak el:

a) előre meghatározott kritériumok és osztályozás alapján értékelést végeznek annak érdekében, hogy meghatározzák a biztonsági események megfékezését és felszámolását célzó intézkedések prioritását;

b) negyedévente megvizsgálják az e rendelet 4. cikkében említett ismétlődő események előfordulását;

c) a biztonsági események értékelése és osztályozása céljából ellenőrzik a vonatkozó naplókat;

d) a naplók összehasonlítására és elemzésére szolgáló eljárást vezetnek be, valamint

e) újraértékelik és átsorolják a biztonsági eseményeket új információ elérhetővé válása esetén, vagy a korábban rendelkezésre álló információk elemzését követően.

3.5. *Biztonsági eseményekre való reagálás*

3.5.1. Az érintett szervezetek a dokumentált eljárásokkal összhangban és kellő időben reagálnak a biztonsági eseményekre.

3.5.2. A biztonsági eseményekre való reagálásra vonatkozó eljárásoknak a következő lépéseket kell magukban foglalniuk:

a) a biztonsági események megfékezése a következmények továbbterjedésének megelőzése érdekében;

b) a biztonsági esemény felszámolása az esemény folytatódásának vagy megismétlődésének megelőzése érdekében;

c) szükség esetén a biztonsági esemény utáni helyreállítás.

3.5.3. Az érintett szervezetek kommunikációs terveket és eljárásokat dolgoznak ki:

a) a számítógép-biztonsági eseményekre reagáló csoportokkal (CSIRT-ek), vagy ha releváns, az illetékes hatóságokkal a biztonsági események bejelentésével kapcsolatban;

b) az érintett szervezet személyzetének tagjaival, valamint az érintett szervezeten kívüli érdekelt felekkel folytatott kommunikációra vonatkozóan.

3.5.4. Az érintett szervezetek a 3.2.1. pontban említett eljárásokkal összhangban naplózzák a biztonsági eseményekre való reagálással kapcsolatos tevékenységeket, és rögzítik a bizonyítékokat.

3.5.5. Az érintett szervezetek tervezett időközönként tesztelik a biztonsági eseményekre való reagálásra vonatkozó eljárásaikat.

3.6. *A biztonsági eseményekkel kapcsolatos utólagos értékelések*

3.6.1. Ha indokolt, az érintett szervezetek a biztonsági események utáni helyreállítást követően utólagos értékelést végeznek. Az utólagos értékelés során lehetőség szerint azonosítani kell az esemény kiváltó okát, és dokumentálni kell a levont tanulságokat az események jövőbeni kialakulásának elhárítása és a következmények enyhítése érdekében.

3.6.2. Az érintett szervezetek gondoskodnak arról, hogy az utólagos értékelések eredményeit felhasználják a szervezet hálózat- és információbiztonsággal, kockázatkezelési intézkedésekkel, valamint a biztonsági események kezelésére, felderítésére és elhárítására irányuló eljárásokkal kapcsolatos megközelítésének javítása céljából.

3.6.3. Az érintett szervezetek tervezett időközönként ellenőrzik, hogy a biztonsági eseményeket követően sor került-e utólagos értékelések elvégzésére.

4. **Üzletmenet-folytonosság és válságkezelés (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének c) pontja)**

4.1. *Üzletmenet-folytonossági és katasztrófa utáni helyreállítási terv*

4.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése c) pontjának alkalmazásában az érintett szervezetek biztonsági események esetén alkalmazandó üzletmenet-folytonossági és katasztrófa-helyreállítási tervet dolgoznak ki és tartanak fenn.

4.1.2. Az érintett szervezetek működését az üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervnek megfelelően helyre kell állítani. A tervnek a 2.1. pont szerint elvégzett kockázatértékelés eredményein kell alapulnia, és ha indokolt, a következőket kell tartalmaznia:

a) cél, hatókör és célcsoport;

b) szerepek és felelősségi körök;

c) kulcsfontosságú kontaktszemélyek és (belső és külső) kommunikációs csatornák;

d) a terv aktiválásának és leállításának feltételei;

e) a műveletek helyreállításának rendje;

f) konkrét műveletekre vonatkozó helyreállítási tervek, beleértve a helyreállítási célkitűzéseket is;

g) a szükséges erőforrások, beleértve a tartalék- és redundáns rendszereket is;

h) a tevékenységek ideiglenes intézkedések révén történő helyreállítása és újraindítása.

4.1.3. Az érintett szervezetek üzletmeneti hatásvizsgálatot végeznek, hogy felmérjék az üzleti tevékenységüket érintő súlyos zavarok lehetséges hatását, és ezen hatásvizsgálat eredményei alapján üzletmenet-folytonossági követelményeket állapítanak meg hálózati és információs rendszereikre vonatkozóan.

4.1.4. Az üzletmenet-folytonossági és a katasztrófa utáni helyreállítási tervet tervezett időközönként, illetve jelentős biztonsági események bekövetkezése, a működést érintő nagyobb változások bevezetése vagy kockázatok felmerülése után tesztelni, értékelni, és ha indokolt, frissíteni kell. Az érintett szervezetek biztosítják, hogy a tervekben felhasználják az említett tesztek eredményeiből levont tanulságokat.

4.2. *Tartalék- és redundáns rendszerek kezelése*

4.2.1. Az érintett szervezetek biztonsági másolatokat tartanak az adatokról, és megfelelő erőforrásokat bocsátanak rendelkezésre – köztük létesítményeket, hálózati és információs rendszereket és személyzetet – a kellő szintű redundáns rendszerek biztosítása érdekében.

4.2.2. A 2.1. pont szerint elvégzett kockázatértékelés eredményei és az üzletmenet-folytonossági terv alapján az érintett szervezetek tartalékrendszerek kezelésére vonatkozó tervet dolgoznak ki, amely a kitér a következőkre:

a) helyreállási idő;

b) annak biztosítása, hogy a biztonsági másolatok teljesek és pontosak legyenek, beleértve a konfigurációs adatokat és a felhőalapú számítástechnikai szolgáltatási környezetben tárolt adatokat;

c) biztonsági másolatok (online vagy offline) tárolása olyan biztonságos helyen vagy helyeken, amelyek nem ugyanabban a hálózatban találhatók, mint a rendszer, és elegendő távolságra vannak ahhoz, hogy ne érintsék őket a fő helyszínen bekövetkező katasztrófákból eredő károk;

d) a biztonsági másolatokhoz való hozzáférés eszközbesorolási szintnek megfelelő fizikai és logikai ellenőrzése;

e) az adatok helyreállítása biztonsági másolatokból;

f) üzleti és szabályozási követelményeken alapuló megőrzési időszakok.

4.2.3. Az érintett szervezetek rendszeresen ellenőrzik a biztonsági másolatok integritását.

4.2.4. A 2.1. pont szerint elvégzett kockázatértékelés eredményei és az üzletmenet-folytonossági terv alapján az érintett szervezetek a következő elemek legalább részleges redundanciája révén biztosítják a megfelelő erőforrások rendelkezésre állását:

a) hálózati és információs rendszerek;

b) eszközök, ideértve a létesítményeket, berendezéseket és felszereléseket;

c) megfelelő szintű felelősséggel, hatáskörrel és szakértelemmel rendelkező személyzet;

d) megfelelő kommunikációs csatornák.

4.2.5. Ha indokolt, az érintett szervezetek biztosítják, hogy a biztonsági tartalék- és redundáns kapacitásra vonatkozó követelményeket megfelelően figyelembe vegyék az erőforrások – többek között a létesítmények, a rendszerek és a személyzet – nyomon követése és az azokat érintő változtatások során.

4.2.6. Az érintett szervezetek rendszeresen tesztelik a biztonsági másolatok helyreállítását és a redundáns rendszerek működését annak biztosítása érdekében, hogy azokra támaszkodva egy esetleges helyreállítási műveletet – a másolatokra, eljárásokra és információkra kiterjedően – hatékonyan végre lehessen hajtani. Az érintett szervezetek dokumentálják a tesztek eredményét, és szükség esetén korrekciós intézkedéseket hoznak.

4.3. *Válságkezelés*

4.3.1. Az érintett szervezetek válságkezelési eljárást vezetnek be.

4.3.2. Az érintett szervezetek biztosítják, hogy a válságkezelési eljárás legalább a következő elemekre kiterjedjen:

a) a személyzet, valamint ha indokolt, a beszállítók és szolgáltatók szerepkörei és felelősségi körei, meghatározva a szerepkörök válsághelyzetekben történő kiosztását, beleértve a követendő konkrét intézkedéseket is;

b) megfelelő kommunikációs eszközök az érintett szervezetek és az érintett illetékes hatóságok között;

c) a hálózati és információs rendszerek biztonságának válsághelyzetekben történő fenntartását biztosító megfelelő intézkedések alkalmazása.

A b) pont alkalmazásában az érintett szervezetek és az érintett illetékes hatóságok közötti információáramlás mind a kötelező kommunikációs elemeket, például a biztonsági esemény jelentését és annak időrendi áttekintését, mind a nem kötelező kommunikációs elemeket magában foglalja.

4.3.3. Az érintett szervezetek a CSIRT-ektől, vagy ha releváns, az illetékes hatóságoktól az eseményekre, sebezhetőségekre, a fenyegetésekre vagy a lehetséges kockázatcsökkentő intézkedésekre vonatkozóan kapott információk kezelésére és felhasználására vonatkozó eljárást vezetnek be.

4.3.4. Az érintett szervezetek rendszeres időközönként, illetve jelentős biztonsági események és a működést érintő nagyobb változásokat követően, vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a válságkezelési tervet.

5. **Az ellátási lánc védelme (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének d) pontja)**

5.1. *Az ellátási lánc védelmére vonatkozó szabályzat*

5.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése d) pontjának alkalmazásában az érintett szervezetek az ellátási lánc védelmére vonatkozó szabályzatot állapítanak meg, hajtanak végre és alkalmaznak, amely a hálózati és információs rendszerek biztonságát érintő azonosított kockázatok csökkentése érdekében szabályozza az érintett szervezetek és közvetlen beszállítóik vagy szolgáltatóik közötti kapcsolatokat. Az ellátási lánc védelmére vonatkozó szabályzatban az érintett szervezetek meghatározzák az ellátási láncban betöltött szerepüket, és erről tájékoztatják közvetlen beszállítóikat és szolgáltatóikat.

5.1.2. Az 5.1.1. pontban említett, az ellátási lánc védelmére vonatkozó szabályzat keretében az érintett szervezetek meghatározzák a beszállítók és szolgáltatók kiválasztására, valamint a velük való szerződéskötésre vonatkozó kritériumokat. A kritériumok a következőket foglalják magukban:

a) a beszállítók és szolgáltatók kiberbiztonsági gyakorlatai, ideértve biztonságos fejlesztési eljárásaikat is;

b) a beszállítók és szolgáltatók azon képessége, hogy megfeleljenek az érintett szervezetek által meghatározott kiberbiztonsági előírásoknak;

c) az IKT-termékek és IKT-szolgáltatások általános minősége és rezilienciája, valamint az azok részét képező kiberbiztonsági kockázatkezelési intézkedések, beleértve az IKT-termékek és IKT-szolgáltatások kockázatait és minősítési szintjét;

d) az érintett szervezetek azon képessége, hogy diverzifikálják a beszerzési forrásokat, és ha releváns, korlátozzák a beszállítóktól való függőséget.

5.1.3. Az ellátási lánc védelmére vonatkozó szabályzat kidolgozása során az érintett szervezetek, ha releváns, figyelembe veszik a kritikus ellátási láncokra vonatkozóan az (EU) 2022/2555 irányelv 22. cikkének (1) bekezdésével összhangban elvégzett összehangolt biztonsági kockázatértékelések eredményeit.

5.1.4. Az érintett szervezetek az ellátási lánc védelmére vonatkozó szabályzatban foglaltak alapján és az e melléklet 2.1. pontjával összhangban elvégzett kockázatértékelés eredményeinek figyelembevételével biztosítják, hogy a beszállítókkal és szolgáltatókkal kötött szerződéseik – ha indokolt – szolgáltatási szintre vonatkozó megállapodások keretében meghatározzák a következőket:

a) a beszállítókra vagy szolgáltatókra vonatkozó kiberbiztonsági követelmények, beleértve az IKT-szolgáltatások vagy IKT-termékek beszerzésének biztonságára vonatkozó, a 6.1. pontban meghatározott követelményeket is;

b) a beszállítók vagy szolgáltatók alkalmazottaival szemben támasztott követelmények azok ismereteit, készségeit és képzését, és ha indokolt, bizonyítványait illetően;

c) a beszállítók és szolgáltatók alkalmazottainak háttérellenőrzésére vonatkozó követelmények;

d) a beszállítók és szolgáltatók azon kötelezettsége, hogy indokolatlan késedelem nélkül értesítsék az érintett szervezeteket minden olyan biztonsági eseménnyel kapcsolatban, amelyek kockázatot jelentenek az említett szervezetek hálózati és információs rendszereinek biztonságára nézve;

e) az ellenőrzés végzésére vagy ellenőrzési jelentés megismerésére való jog;

f) a beszállítók és szolgáltatók azon kötelezettsége, hogy kezeljék az érintett szervezetek hálózati és információs rendszereinek biztonságát veszélyeztető sebezhetőségeket;

g) az alvállalkozásba adásra vonatkozó követelmények, valamint – amennyiben az érintett szervezetek lehetővé teszik alvállalkozói szerződések megkötését – az alvállalkozókkal szemben támasztott kiberbiztonsági követelmények az a) pontban említett kiberbiztonsági követelményekkel összhangban;

h) a beszállítók és szolgáltatók kötelezettségei a szerződés megszűnésekor, például a beszállítók és szolgáltatók által feladataik ellátása során megszerzett információk visszakeresésével és megsemmisítésével kapcsolatban.

5.1.5. Az érintett szervezetek az új beszállítók és szolgáltatók kiválasztási folyamata, valamint a 6.1. pontban említett közbeszerzési eljárás során figyelembe veszik az 5.1.2. és az 5.1.3. pontban említett elemeket.

5.1.6. Az érintett szervezetek tervezett időközönként, illetve a működést érintő nagyobb változásokat követően, kockázatok felmerülése esetén, valamint az IKT-szolgáltatások nyújtásával kapcsolatos vagy a beszállítók és szolgáltatók által kínált IKT-termékek biztonságát érintő jelentős biztonsági események bekövetkezte esetén felülvizsgálják az ellátási lánc védelmére vonatkozó szabályzatot, valamint megvizsgálják, értékelik a beszállítók és szolgáltatók kiberbiztonsági gyakorlataiban bekövetkező változásokat, és szükség esetén megfelelő intézkedéseket hoznak.

5.1.7. Az 5.1.6. pont alkalmazásában az érintett szervezetek:

a) ha releváns, rendszeresen nyomon követik a szolgáltatási szintre vonatkozó megállapodások végrehajtásáról szóló jelentéseket;

b) felülvizsgálják a beszállítók és szolgáltatók által biztosított IKT-termékekkel és IKT-szolgáltatásokkal kapcsolatos biztonsági eseményeket;

c) felmérik a nem tervezett felülvizsgálatok szükségességét, és átfogó módon dokumentálják a megállapításokat;

d) elemzik a beszállítók és szolgáltatók által biztosított IKT-termékekkel és IKT-szolgáltatásokkal kapcsolatos változásokból eredő kockázatokat, és ha indokolt, időben meghozzák a kockázatcsökkentő intézkedéseket.

5.2. *Beszállítók és szolgáltatók jegyzéke*

Az érintett szervezetek nyilvántartást vezetnek és tartanak naprakészen közvetlen beszállítóikról és szolgáltatóikról, amely többek között a következőket tartalmazza:

a) a közvetlen beszállítók és szolgáltatók kapcsolattartói;

b) az értinett szervezet számára a közvetlen szállító vagy szolgáltató által biztosított IKT-termékek, IKT-szolgáltatások és IKT-eljárások jegyzéke.

6. **A hálózati és információs rendszerek biztonságos beszerzése, fejlesztése és karbantartása (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének e) pontja)**

6.1. *IKT-szolgáltatások vagy IKT-termékek biztonságos beszerzése*

6.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése e) pontjának alkalmazásában az érintett szervezetek a 2.1. pont szerint elvégzett kockázatértékelés alapján eljárásokat határoznak meg és hajtanak végre az érintett szervezetek hálózati és információs rendszereinek biztonsága szempontjából kritikus elemek tekintetében a beszállítóktól vagy szolgáltatóktól beszerzett IKT-szolgáltatásokból vagy IKT-termékekből eredő kockázatok kezelésére azok teljes életciklusa során.

6.1.2. A 6.1.1. pont alkalmazásában a 6.1.1. pontban említett eljárások a következőket foglalják magukban:

a) a beszerzendő IKT-szolgáltatásokra vagy IKT-termékekre alkalmazandó biztonsági követelmények;

b) az IKT-szolgáltatások vagy IKT-termékek teljes életciklusa alatti biztonsági frissítésekre, illetve a támogatási időszak végét követő cserére vonatkozó követelmények;

c) az IKT-szolgáltatásokban vagy IKT-termékekben használt hardver- és szoftverelemekre vonatkozó információk;

d) az IKT-szolgáltatások vagy IKT-termékek telepített kiberbiztonsági funkcióira és a biztonságos működésükhöz szükséges konfigurációra vonatkozó információk;

e) annak biztosítása, hogy az IKT-szolgáltatások vagy IKT-termékek megfelelnek az a) pontban említett biztonsági követelményeknek;

f) az annak hitelesítésére szolgáló módszerek, hogy a biztosított IKT-szolgáltatások vagy IKT-termékek megfelelnek-e a meghatározott biztonsági követelményeknek, valamint a validálási eredmények dokumentálása.

6.1.3. Az érintett szervezetek tervezett időközönként és jelentős biztonsági események bekövetkezése esetén felülvizsgálják, és ha indokolt, frissítik az eljárásokat.

6.2. *Biztonságos fejlesztési életciklus*

6.2.1. A hálózati és információs rendszerek – ezen belül a szoftverek – fejlesztését megelőzően az érintett szervezetek szabályokat állapítanak meg a hálózati és információs rendszerek biztonságos fejlesztésére vonatkozóan, amelyeket a hálózati és információs rendszerek belső fejlesztésekor vagy a hálózati és információs rendszerek fejlesztésének kiszervezésekor kell alkalmazni. A szabályoknak a fejlesztés valamennyi szakaszára ki kell terjedniük, beleértve a specifikációt, a tervezést, a fejlesztést, a végrehajtást és a tesztelést is.

6.2.2. A 6.2.1. pont alkalmazásában az érintett szervezetek:

a) az érintett szervezetek által vagy nevükben végzett fejlesztési vagy beszerzési projektek specifikációs és tervezési szakaszában elvégzik a biztonsági követelmények elemzését;

b) az információs rendszerek fejlesztését érintő tevékenységekkel kapcsolatban a biztonságos rendszertervezésre és a biztonságos kódolásra vonatkozó alapelveket alkalmaznak, ideértve a beépített kiberbiztonság és a „zéró bizalom” architektúrák előmozdítását;

c) a fejlesztési környezetre vonatkozó biztonsági követelményeket állapítanak meg;

d) biztonsági tesztelési eljárásokat dolgoznak ki és hajtanak végre a fejlesztési ciklusban;

e) gondoskodnak a biztonsági tesztadatok megfelelő kiválasztásáról, védelméről és kezeléséről;

f) a 2.1. pont szerint elvégzett kockázatértékelésnek megfelelően biztonságosan megsemmisítik és anonimizálják a tesztadatokat.

6.2.3. A hálózati és információs rendszerek fejlesztésének kiszervezése esetén az érintett szervezetek az 5. és a 6.1. pontban említett szabályzatokat és eljárásokat is alkalmazzák.

6.2.4. Az érintett szervezetek tervezett időközönként felülvizsgálják és szükség esetén frissítik a biztonságos fejlesztésre vonatkozó szabályaikat.

6.3. *Konfigurációkezelés*

6.3.1. Az érintett szervezetek megteszik a megfelelő intézkedéseket a konfigurációk – többek között a hardver-, szoftver-, szolgáltatás- és hálózatbiztonsági konfigurációk – megállapítása, dokumentálása, alkalmazása és nyomon követése érdekében.

6.3.2. A 6.3.1. pont alkalmazásában az érintett szervezetek:

a) gondoskodnak a hardverek, szoftverek, szolgáltatások és hálózatok konfigurációinak biztonságossá tételéről és védelméről;

b) eljárásokat és eszközöket dolgoznak ki és alkalmaznak a hardverek, szoftverek, szolgáltatások és hálózatok tekintetében meghatározott biztonsági konfigurációik használatának ellenőrzésére mind az újonnan telepített rendszerek, mind pedig a már üzemben lévő rendszerek esetében, azok teljes életciklusa alatt.

6.3.3. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a konfigurációkat.

6.4. *Változáskezelés, javítás és karbantartás*

6.4.1. A hálózati és információs rendszerek változásainak ellenőrzése érdekében az érintett szervezetek változáskezelési eljárásokat alkalmaznak. Ha releváns, az eljárásoknak összhangban kell állniuk az érintett szervezetek változáskezelésre vonatkozó általános szabályaival.

6.4.2. A 6.4.1. pontban említett eljárásokat az üzemben lévő szoftverek és hardverek új verzióira, módosítására és vészhelyzeti változtatásaira, valamint a konfiguráció-módosításokra kell alkalmazni. Az eljárásoknak biztosítaniuk kell, hogy a változásokat dokumentálják, és lehetséges hatásaikat végrehajtásuk előtt a 2.1. ponttal összhangban elvégzett kockázatértékelés alapján teszteljék és értékeljék.

6.4.3. Amennyiben valamilyen vészhelyzet miatt nincs lehetőség a szokásos változáskezelési eljárások alkalmazására, az érintett szervezeteknek dokumentálniuk kell a változás eredményét és magyarázatot kell adniuk arra, hogy az eljárásokat miért nem lehetett alkalmazni.

6.4.4. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik az eljárásokat.

6.5. *Biztonsági tesztelés*

6.5.1. Az érintett szervezetek biztonsági tesztelésre vonatkozó szabályzatot és eljárásokat dolgoznak ki, hajtanak végre és alkalmaznak.

6.5.2. Az érintett szervezetek:

a) a 2.1. pont szerint elvégzett kockázatértékelés alapján megállapítják a biztonsági tesztek elvégzésének szükségességét, hatókörét, gyakoriságát és típusát;

b) dokumentált vizsgálati módszertannak megfelelően biztonsági teszteket végeznek azokon a rendszerelemeken, amelyeket a kockázatelemzés a biztonságos működés szempontjából relevánsnak minősített;

c) dokumentálják a tesztek típusát, hatókörét, idejét és eredményeit, beleértve az egyes megállapításokra vonatkozó kritikusság értékelését és kockázatcsökkentő intézkedéseket;

d) kritikusnak minősülő megállapítások esetén kockázatcsökkentő intézkedéseket alkalmaznak.

6.5.3. Az érintett szervezetek tervezett időközönként felülvizsgálják, és ha indokolt, frissítik biztonsági tesztelésre vonatkozó szabályaikat.

6.6. *Biztonsági javítások kezelése*

6.6.1. Az érintett szervezetek olyan eljárásokat határoznak meg és alkalmaznak, amelyek összhangban vannak a 6.4.1. pontban említett változáskezelési eljárásokkal, valamint a sebezhetőségkezelési, kockázatkezelési és egyéb vonatkozó eljárásokkal. Ezen eljárások célja annak biztosítása, hogy:

a) a biztonsági javítások elérhetővé válásukat követően, észszerű időn belül alkalmazásra kerüljenek;

b) a biztonsági javításokat a gyártási rendszerekben való alkalmazás előtt teszteljék;

c) a biztonsági javítások megbízható forrásokból származzanak, és azok integritását ellenőrizzék;

d) további intézkedéseket hajtanak végre és elfogadják a fennmaradó kockázatokat abban az esetben, ha nem áll rendelkezésre javítás, vagy nem kerül sor a javítás 6.6.2. pont szerinti alkalmazására.

6.6.2. A 6.6.1. a) ponttól eltérve az érintett szervezetek dönthetnek úgy, hogy nem alkalmaznak biztonsági javításokat, amennyiben a biztonsági javítás alkalmazásával járó hátrányok meghaladnák a kiberbiztonsági szempontból várható előnyöket. Az érintett szervezetek megfelelően dokumentálják és megindokolják az ilyen döntéseiket.

6.7. *Hálózatbiztonság*

6.7.1. Az érintett szervezetek megteszik a megfelelő intézkedéseket hálózati és információs rendszereik kiberfenyegetésekkel szembeni védelme érdekében.

6.7.2. A 6.7.1. pont alkalmazásában az érintett szervezetek:

a) részletes dokumentációt vezetnek a hálózat architektúrájáról és azt naprakészen tartják;

b) az érintett szervezet belső hálózati területeinek jogosulatlan hozzáféréssel szembeni védelmét szolgáló ellenőrzéseket vezetnek be és hajtanak végre;

c) olyan ellenőrzéseket dolgoznak ki, amelyek megakadályozzák az érintett szervezetek működése szempontjából nem feltétlenül szükséges hozzáférést és hálózati csatlakozást;

d) meghatározzák és alkalmazzák a hálózati és információs rendszerekhez való távoli hozzáférésre vonatkozó, a szolgáltatók hozzáférésére is kiterjedő ellenőrzéseket;

e) a biztonsági szabályzat végrehajtásának irányítására használt rendszereket nem használják más célokra;

f) kifejezetten tiltják vagy lekapcsolják a szükségtelen csatlakozásokat és szolgáltatásokat;

g) ha indokolt, kizárólag az érintett szervezetek által engedélyezett eszközök számára engedélyezik az érintett szervezet hálózati és információs rendszereihez való hozzáférést;

h) szolgáltatók számára csak engedélykérelem benyújtását követően és csak meghatározott időtartamra – például karbantartási művelet időtartamára – engedélyezik a csatlakozást;

i) biztosítják, hogy a különböző rendszerek közötti kommunikációra kizárólag olyan megbízható csatornákon keresztül kerüljön sor, amelyek logikai, kriptográfiai módon vagy fizikailag elszigeteltek más kommunikációs csatornáktól, és amelyek esetében biztosított a végberendezéseik azonosítása, valamint az adott csatornán átfutó adatok módosítással vagy a nyilvánosságra hozatallal szembeni védelme;

j) végrehajtási tervet fogadnak el a legújabb generációs, hálózati rétegbeli kommunikációs protokollokra való biztonságos, megfelelő és fokozatos átállásra vonatkozóan, és intézkedéseket hoznak az átállás felgyorsítására;

k) végrehajtási tervet fogadnak el az elektronikus levelezésre vonatkozó, nemzetközileg elfogadott és interoperábilis, modern kommunikációs szabványok bevezetésére vonatkozóan, hogy az e-mailes fenyegetésekhez kapcsolódó sebezhetőségek enyhítése révén biztonságossá váljon az elektronikus levelezés, és intézkedéseket hoznak a bevezetés felgyorsítására;

l) a DNS-biztonsággal, valamint az internetes útvonal-meghatározás biztonságával és az útvonal-meghatározási higiéniával kapcsolatos bevált gyakorlatokat alkalmaznak.

6.7.3. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik az említett intézkedéseket.

6.8. *Hálózati szegmentáció*

6.8.1. Az érintett szervezetek a 2.1. pontban említett kockázatértékelés eredményeivel összhangban hálózatokra vagy zónákra bontják rendszereiket. A szegmentálás révén leválasztják rendszereiket és hálózataikat a harmadik felek rendszereiről és hálózatairól.

6.8.2. Ennek keretében az érintett szervezetek:

a) figyelembe veszik a megbízható rendszerek és szolgáltatások közötti funkcionális, logikai és fizikai kapcsolatot, beleértve azok helyszínét is;

b) az egyes hálózatokhoz vagy zónákhoz a biztonsági követelmények értékelése alapján biztosítanak hozzáférést;

c) az érintett szervezet működése vagy a biztonság szempontjából kritikus rendszereket biztonságos zónákban tartják;

d) kommunikációs hálózataikon belül demilitarizált övezetet hoznak létre az érintett szervezet hálózataiból kiinduló vagy oda irányuló kommunikáció védelmének biztosítása érdekében;

e) a zónák között és azokon belül a hozzáférést és kommunikációt az érintett szervezetek működéséhez vagy a biztonsághoz szükséges mértékre korlátozzák;

f) leválasztják a hálózati és információs rendszerek irányítására szolgáló hálózatot az érintett szervezetek operatív hálózatáról;

g) elkülönítik a hálózati adminisztrációs csatornákat a többi hálózati forgalomtól;

h) leválasztják az érintett szervezetek által végzett szolgáltatások számára fenntartott rendszereket a fejlesztés és tesztelés során használt rendszerekről, ideértve a biztonsági tartalékrendszereket is.

6.8.3. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, módosítják a hálózatok szegmentációját.

6.9. *A rosszindulatú és nem engedélyezett szoftverekkel szembeni védelem*

6.9.1. Az érintett szervezetek védik hálózati és információs rendszereiket a rosszindulatú és nem engedélyezett szoftverekkel szemben.

6.9.2. E célból az érintett szervezetek különösen olyan intézkedéseket hajtanak végre, amelyek észlelik vagy megakadályozzák a rosszindulatú vagy nem engedélyezett szoftverek használatát. Ha indokolt, az érintett szervezetek biztosítják, hogy hálózati és információs rendszereik fel legyenek szerelve az említett szoftvereket észlelő és azokra reagáló szoftverrel, amelyet a 2.1. pont szerint elvégzett kockázatértékelésnek és a szolgáltatókkal kötött szerződéses megállapodásoknak megfelelően rendszeresen frissítenek.

6.10. *A sebezhetőségek kezelése és feltárása*

6.10.1. Az érintett szervezetek információkat gyűjtenek a hálózati és információs rendszereiket érintő műszaki sebezhetőségekről, értékelik az ilyen sebezhetőségeknek való kitettségüket, és megfelelő intézkedéseket hoznak a sebezhetőségek kezelésére.

6.10.2. A 6.10.1. pont alkalmazásában az érintett szervezetek:

a) megfelelő csatornákon keresztül, például a CSIRT-ek, az illetékes hatóságok bejelentései vagy a beszállítók és szolgáltatók által szolgáltatott adatok révén figyelemmel kísérik a sebezhetőségekkel kapcsolatos információkat;

b) ha indokolt, tervezett időközönként sérülékenységfelméréseket végeznek, és rögzítik a felmérés eredményeit;

c) haladéktalanul megkezdik az érintett szervezet által saját működése szempontjából kritikusnak minősített sebezhetőségek kezelését;

d) biztosítják, hogy sebezhetőség kezelésére vonatkozó eljárásaik összhangban álljanak a változások, a biztonsági javítások, a kockázatok és a biztonsági események kezelésére vonatkozó eljárásaikkal;

e) az alkalmazandó nemzeti összehangolt sebezhetőség-feltárási szabályzattal összhangban meghatározzák a sebezhetőségek feltárására vonatkozó eljárásukat.

6.10.3. Amennyiben a sebezhetőség potenciális hatása azt indokolja, az érintett szervezetek a sebezhetőség mérséklésére szolgáló tervet dolgoznak ki és hajtanak végre. Más esetekben az érintett szervezetek dokumentálják és megokolják, hogy a sebezhetőség miért nem igényel korrekciós intézkedést.

6.10.4. Az érintett szervezetek tervezett időközönként felülvizsgálják, és ha indokolt, frissítik a sebezhetőségekkel kapcsolatos információk nyomon követésére használt csatornákat.

7. **Szabályzat és eljárások a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének f) pontja)**

7.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése f) pontjának alkalmazásában az érintett szervezetek szabályzatot és eljárásokat dolgoznak ki, hajtanak végre és alkalmaznak annak értékelésére, hogy az érintett szervezet által hozott kiberbiztonsági kockázatkezelési intézkedéseket hatékonyan hajtják-e végre és tartják-e fenn.

7.2. A 7.1. pontban említett szabályzatnak és eljárásoknak figyelembe kell venniük a 2.1. pont szerinti kockázatértékelés eredményeit és a múltbeli jelentős eseményeket. Az érintett szervezetek meghatározzák a következőket:

a) mely kiberbiztonsági kockázatkezelési intézkedéseket kell nyomon követni és mérni, beleértve a folyamatokat és ellenőrzéseket is;

b) nyomonkövetési, mérési, elemzési és értékelési módszerek, szükség szerint, az érvényes eredmények biztosítása érdekében;

c) mikor kell elvégezni a nyomon követést és a mérést;

d) ki felel a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának nyomon követéséért és méréséért;

e) mikor kell elemezni és értékelni a nyomon követési és mérési eredményeket;

f) kinek kell elemeznie és értékelnie a szóban forgó eredményeket.

7.3. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a szabályzatot és az eljárásokat.

8. **Alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzés (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének g) pontja)**

8.1. *Tájékoztatás és alapvető kiberhigiéniai gyakorlatok*

8.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése g) pontjának alkalmazásában az érintett szervezetek biztosítják, hogy alkalmazottaik, köztük a vezető testületek tagjai, valamint a közvetlen beszállítók és szolgáltatók tisztában legyenek a kockázatokkal, tájékoztatást kapjanak a kiberbiztonság fontosságáról, és kiberhigiéniai gyakorlatokat alkalmazzanak.

8.1.2. A 8.1.1. pont alkalmazásában az érintett szervezetek olyan tájékoztató programot kínálnak alkalmazottaik részére – beleértve a vezető testületek tagjait is –, valamint ha indokolt, az 5.1.4. ponttal összhangban a közvetlen beszállítók és szolgáltatók részére, amelynek:

a) rendszeresen kell ismétlődnie, hogy azon az új alkalmazottak részt vehessenek;

b) összhangban kell lennie a hálózat- és információbiztonsági szabályzattal, a tematikus szabályzattal és a hálózat- és információbiztonsági eljárásokkal;

c) ki kell terjednie a releváns kiberfenyegetésekre, az érvényben lévő kiberbiztonsági kockázatkezelési intézkedésekre, a kapcsolattartó pontokra és a kiberbiztonsági kérdésekkel kapcsolatos további információkhoz és tanácsadáshoz szükséges erőforrásokra, valamint a felhasználók kiberhigiéniai gyakorlataira.

8.1.3. A tájékoztató programot, ha indokolt, hatékonysági szempontból tesztelni kell. A tájékoztató programot tervezett időközönként kell kínálni és frissíteni a kiberhigiéniai gyakorlatok változásainak, az aktuális fenyegetettségi helyzetnek és az érintett szervezeteket fenyegető kockázatoknak a figyelembevételével.

8.2. *Kiberbiztonsági képzés*

8.2.1. Az érintett szervezetek azonosítják azokat az alkalmazottakat, akiknek a szerepköre biztonsági szempontból releváns készségeket és szakértelmet igényel, és biztosítják, hogy rendszeres képzésben részesüljenek a hálózati és információs rendszerek biztonsága terén.

8.2.2. Az érintett szervezetek a hálózat- és információbiztonsági szabályzattal, a tematikus szabályzattal és a hálózat- és információbiztonsággal kapcsolatos egyéb vonatkozó eljárásokkal összhangban képzési programot dolgoznak ki, hajtanak végre és alkalmaznak, amelyben bizonyos kritériumok alapján meghatározzák az egyes szerepkörök és pozíciók képzési igényeit.

8.2.3. A 8.2.1. pontban említett képzésnek relevánsnak kell lennie az alkalmazott munkaköri funkciója szempontjából; a képzés hatékonyságát ki kell értékelni. A képzésnek figyelembe kell vennie a meglévő biztonsági intézkedéseket, és ki kell terjednie a következőkre:

a) a hálózati és információs rendszerek, köztük a mobil eszközök biztonságos konfigurálásával és működtetésével kapcsolatos utasítások;

b) tájékoztatás az ismert kiberfenyegetésekről;

c) a biztonsági szempontból releváns események bekövetkezésekor tanúsított magatartásra vonatkozó képzés.

8.2.4. Az érintett szervezetek képzést szerveznek a személyzet azon tagjai számára, akiket olyan új pozíciókba vagy munkakörökbe helyeznek át, amelyek biztonsági szempontból releváns készségeket és szakértelmet igényelnek.

8.2.5. A programot rendszeres időközönként kell kínálni és frissíteni az alkalmazandó szabályzat és szabályok, az adott szerepkörök és felelősségi körök, valamint az ismert kiberfenyegetések és technológiai fejlemények figyelembevételével.

9. **Kriptográfia (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének h) pontja)**

9.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése h) pontjának alkalmazásában az érintett szervezetek kriptográfiai szabályzatot és eljárásokat dolgoznak ki, hajtanak végre és alkalmaznak annak érdekében, hogy biztosítsák a kriptográfia megfelelő és hatékony használatát az adatok bizalmas jellegének, hitelességének és integritásának védelme érdekében, összhangban az érintett szervezetek eszközminősítésével és a 2.1. pont szerint elvégzett kockázatértékelés eredményeivel.

9.2. A 9.1. pontban említett szabályzatnak és eljárásoknak meg kell határozniuk a következőket:

a) az érintett szervezetek eszközminősítésével összhangban az érintett szervezetek eszközeinek védelméhez szükséges kriptográfiai intézkedések típusa, erőssége és minősége, beleértve az inaktív és átvitel alatt lévő adatokat is;

b) az a) pont alapján az elfogadandó protokollok vagy protokollcsaládok, valamint a kriptográfiai algoritmusok, a titkosítás erőssége, a kriptográfiai megoldások és az érintett szervezetek által jóváhagyandó és megkövetelt felhasználási gyakorlatok, ha indokolt, kriptográfiai agilitási megközelítés alkalmazásával;

c) az érintett szervezeteknek a rejtjelkulcsok kezelésével kapcsolatos megközelítése, beleértve – ha indokolt – a következőkre vonatkozó módszereket:

i. különféle rejtjelkulcsok létrehozása kriptográfiai rendszerekhez és alkalmazásokhoz;

ii. rejtjelkulcs-tanúsítványok kiállítása és megszerzése;

iii. rejtjelkulcsok kiosztása a kijelölt szervezetek között, beleértve a kulcsok átvételt követő aktiválásának módját is;

iv. rejtjelkulcsok tárolása, beleértve azt is, hogy az engedéllyel rendelkező felhasználók hogyan férnek hozzá a kulcsokhoz;

v. rejtjelkulcsok módosítása vagy frissítése, beleértve a kulcsok módosításának idejére és módjára vonatkozó szabályokat is;

vi. veszélyeztetett rejtjelkulcsok kezelése;

vii. rejtjelkulcsok visszavonása, beleértve a kulcsok visszavonásának vagy deaktiválásának módját is;

viii. elveszett vagy sérült rejtjelkulcsok visszanyerése;

ix. rejtjelkulcsok rögzítése vagy archiválása;

x. rejtjelkulcsok megsemmisítése;

xi. a rejtjelkulcs-kezeléssel kapcsolatos tevékenységek naplózása és ellenőrzése;

xii. a rejtjelkulcsok aktiválási és deaktiválási időpontjainak meghatározása, biztosítva, hogy a kulcsokat a szervezet rejtjelkulcs-kezelésre vonatkozó szabályainak megfelelően csak meghatározott ideig lehessen használni.

9.3. Az érintett szervezetek tervezett időközönként felülvizsgálják, és ha indokolt, frissítik a szabályzatot és az eljárásokat, figyelemmel a legújabb technikai lehetőségekre a kriptográfia terén.

10. **Humánerőforrás-biztonság (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének i) pontja)**

10.1. *Humánerőforrás-biztonság*

10.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése i) pontjának alkalmazásában az érintett szervezetek biztosítják, hogy alkalmazottaik, valamint adott esetben a közvetlen beszállítók és szolgáltatók megértsék biztonsági feladataikat és elkötelezzék magukat azok elvégzése mellett a kínált szolgáltatásoknak és a munkakörnek megfelelően és az érintett szervezeteknek a hálózati és információs rendszerek biztonságára vonatkozó szabályzatával összhangban.

10.1.2. A 10.1.1. pontban említett követelménynek a következőket kell tartalmaznia:

a) mechanizmusok annak biztosítására, hogy valamennyi alkalmazott, valamint adott esetben közvetlen beszállító és szolgáltató megértse és kövesse azokat a standard kiberhigiéniai gyakorlatokat, amelyeket az érintett szervezetek a 8.1. pont értelmében alkalmaznak;

b) mechanizmusok annak biztosítására, hogy valamennyi adminisztratív vagy kiemelt hozzáféréssel rendelkező felhasználó tisztában legyen a szerepkörével, felelősségi körével és hatáskörével, és annak megfelelően járjon el;

c) mechanizmusok annak biztosítására, hogy a vezető testületek tagjai megértsék a hálózati és információs rendszerek biztonságával kapcsolatos szerepkörüket, felelősségi köreiket és hatáskörüket, és azoknak megfelelően járjanak el;

d) az egyes munkakörök tekintetében a képzett személyzet felvételére szolgáló mechanizmusok, például referenciaellenőrzések, átvilágítási eljárások, tanúsítványok validálása vagy írásbeli vizsgák.

10.1.3. Az érintett szervezetek tervezett időközönként, de legalább évente felülvizsgálják a személyzetnek az 1.2. pont szerinti meghatározott szerepkörökbe történő beosztását, valamint az emberi erőforrások e tekintetben történő felhasználását. A feladatkörökbe történő beosztást szükség esetén frissíteni kell.

10.2. *Háttérellenőrzés*

10.2.1. Ha megvalósítható, az érintett szervezetek gondoskodnak saját alkalmazottaik, valamint ha releváns, az 5.1.4. ponttal összhangban a közvetlen beszállítók és szolgáltatók háttérellenőrzéséről, amennyiben ez az érintett személyek szerepköre, felelősségi köre és hatásköre miatt szükséges.

10.2.2. Az 10.2.1. pont alkalmazásában az érintett szervezetek:

a) kritériumokat vezetnek be, amelyek meghatározzák, hogy mely szerepköröket, felelősségi köröket és hatásköröket gyakorolhatják kizárólag olyan személyek, akik háttérellenőrzésen estek át;

b) gondoskodnak arról, hogy a szóban forgó személyek háttérellenőrzését e szerepkörök, felelősségi körök és hatáskörök gyakorlásának megkezdése előtt a 10.2.1. pont szerint elvégezzék, mely háttérellenőrzés során az üzleti követelményekkel arányosan figyelembe kell venni az alkalmazandó törvényeket, rendeleteket és etikát, a 12.1. pontban említett eszközminősítést, a hozzáférhető hálózati és információs rendszereket, valamint az észlelt kockázatokat.

10.2.3. Az érintett szervezetek tervezett időközönként felülvizsgálják, és ha indokolt, frissítik a szabályzatot.

10.3. *A foglalkoztatási eljárások megszüntetése vagy megváltoztatása*

10.3.1. Az érintett szervezetek gondoskodnak arról, hogy a hálózat- és információs rendszerek biztonságával kapcsolatos azon felelősségek és kötelezettségek, amelyek alkalmazottaik foglalkoztatásának megszűnését vagy megváltozását követően is érvényben maradnak, szerződésben kerüljenek meghatározásra és érvényesítésre.

10.3.2. A 10.3.1. pont alkalmazásában az érintett szervezetek az egyén foglalkoztatási feltételeibe, szerződéseibe vagy megállapodásaiba belefoglalják azokat a felelősségi köröket és kötelezettségeket, amelyek a foglalkoztatás vagy a szerződés megszűnését követően is érvényben vannak, ilyen például a titoktartási záradék.

10.4. *Fegyelmi eljárás*

10.4.1. Az érintett szervezetek fegyelmi eljárást hoznak létre, tesznek közzé és tartanak fenn a hálózati és információs rendszerekre vonatkozó biztonsági szabályzat megsértésének kezelésére. Az eljárás során figyelembe kell venni a vonatkozó jogi, jogszabályi, szerződéses és üzleti követelményeket.

10.4.2. Az érintett szervezetek tervezett időközönként, amennyiben ezt jogszabályi változások szükségessé teszik, illetve a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a fegyelmi eljárást.

11. **Hozzáférés-ellenőrzés (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének i) és j) pontja)**

11.1. *Hozzáférés-ellenőrzési szabályzat*

11.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése i) pontjának alkalmazásában az érintett szervezetek az üzleti követelmények, valamint a hálózat- és információs rendszer biztonsági követelményei alapján logikai és fizikai hozzáférés-ellenőrzési szabályzatot dolgoznak ki, dokumentálnak és hajtanak végre a hálózati és információs rendszereikhez való hozzáférés tekintetében.

11.1.2. A 11.1.1. pontban említett szabályzatnak:

a) kezelnie kell a személyek, köztük a személyzet, a látogatók és a külső szervezetek, például a beszállítók és szolgáltatók hozzáférését;

b) kezelnie kell a hálózati és információs rendszerek hozzáférését;

c) biztosítania kell, hogy csak megfelelően hitelesített felhasználók kapjanak hozzáférést.

11.1.3. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a szabályzatot.

11.2. *A hozzáférési jogok kezelése*

11.2.1. Az érintett szervezetek a hálózati és információs rendszerekhez való hozzáférési jogokat a 11.1. pontban említett hozzáférés-ellenőrzési szabályzattal összhangban biztosítják, módosítják, megszüntetik és dokumentálják.

11.2.2. Az érintett szervezetek:

a) a hozzáférési jogokat kijelölik és visszavonják a szükséges ismeret elve, a legkisebb kiváltság elve és a feladatszétválasztás elve alapján;

b) a foglalkoztatás megszűnése vagy megváltozása esetén biztosítják a hozzáférési jogok ennek megfelelő módosítását;

c) biztosítják, hogy a releváns személyek engedélyezzék a hálózati és információs rendszerekhez való hozzáférést;

d) biztosítják harmadik felek – például látogatók, beszállítók és szolgáltatók – hozzáférési jogainak megfelelő kezelését, különösen a hozzáférési jogok hatályának és időtartamának korlátozásával;

e) nyilvántartást vezetnek a megadott hozzáférési jogokról;

f) naplózást alkalmaznak a hozzáférési jogok kezelésére.

11.2.3. Az érintett szervezetek tervezett időközönként felülvizsgálják a hozzáférési jogokat, és a szervezeti változások alapján módosítják azokat. Az érintett szervezetek dokumentálják a felülvizsgálat eredményeit, beleértve a hozzáférési jogok szükséges módosításait is.

11.3. *Különleges jogosultságú vagy rendszeradminisztrátori felhasználói fiókok*

11.3.1. Az érintett szervezetek a 11.1. pontban említett hozzáférés-ellenőrzési szabályzat részeként szabályzatot tartanak fenn a különleges jogosultságú vagy rendszeradminisztrátori felhasználói fiókok kezelésére.

11.3.2. A 11.3.1. pontban említett szabályzatnak:

a) biztosítania kell a megbízható azonosítást és hitelesítést, például többtényezős hitelesítés révén, valamint engedélyezési eljárásokat kell létrehoznia a különleges jogosultságú vagy rendszeradminisztrátori felhasználói fiókok tekintetében;

b) biztosítania kell külön fiókok létrehozását kizárólag a rendszeradminisztrációs műveletek – például telepítés, konfigurálás, kezelés vagy karbantartás – céljára;

c) biztosítania kell a rendszeradminisztrációs jogosultságok lehető legnagyobb mértékű egyénre szabását és korlátozását,

d) biztosítania kell, hogy a rendszeradminisztrációs fiókokat csak a rendszeradminisztrációs rendszerekhez történő csatlakozásra használják.

11.3.3. Az érintett szervezetek tervezett időközönként felülvizsgálják a különleges jogosultságú vagy rendszeradminisztrátori felhasználói fiókokhoz való hozzáférési jogokat, és a szervezeti változások alapján módosítják azokat, valamint dokumentálják a felülvizsgálat eredményeit, beleértve a hozzáférési jogok szükséges módosításait is.

11.4. *Adminisztrációs rendszerek*

11.4.1. Az érintett szervezetek az adminisztrációs rendszerek használatát a 11.1. pontban említett hozzáférés-ellenőrzési szabályzattal összhangban korlátozzák és felügyelik.

11.4.2. E célból az érintett szervezetek:

a) a rendszeradminisztrációs rendszereket csak rendszeradminisztrációs célokra használják, egyéb műveletekhez nem;

b) az ilyen rendszereket logikailag elkülönítik a rendszeradminisztrációs célokra nem használt alkalmazásszoftverektől;

c) hitelesítés és titkosítás révén biztosítják a rendszeradminisztrációs rendszerekhez való hozzáférés védelmét.

11.5. *Azonosítás*

11.5.1. Az érintett szervezetek kezelik a hálózati és információs rendszerek és felhasználóik azonosító adatainak (azonosítóinak) teljes életciklusát.

11.5.2. E célból az érintett szervezetek:

a) a hálózati és információs rendszerek és felhasználóik számára egyedi azonosítókat hoznak létre;

b) a felhasználói azonosítót egyetlen személyhez kapcsolják;

c) biztosítják a hálózati és információs rendszerek azonosítóinak felügyeletét;

d) naplózást alkalmaznak az azonosítók kezelésére.

11.5.3. Az érintett szervezetek csak akkor engedélyeznek több személyhez rendelt azonosítókat, például megosztott azonosítókat, ha azok üzleti vagy működési okokból szükségesek, és ha azok kifejezett jóváhagyási eljárás és dokumentáció tárgyát képezik. Az érintett szervezetek a 2.1. pontban említett kiberbiztonsági kockázatkezelési keretrendszerben figyelembe veszik a több személyhez rendelt azonosítókat.

11.5.4. Az érintett szervezetek rendszeresen felülvizsgálják a hálózati és információs rendszerek és felhasználóik azonosítóit, és amennyiben azokra már nincs szükség, azokat haladéktalanul deaktiválják.

11.6. *Hitelesítés*

11.6.1. Az érintett szervezetek a hozzáférési korlátozásokon és a hozzáférés-ellenőrzési szabályzaton alapuló biztonságos hitelesítési eljárásokat és technológiákat hajtanak végre.

11.6.2. E célból az érintett szervezetek:

a) biztosítják, hogy a hitelesítés foka megfeleljen a hozzáféréssel elérni kívánt eszköz minősítésének;

b) felügyelik a titkos hitelesítési információk felhasználók közötti kiosztását és kezelését az információk bizalmas kezelését biztosító folyamat révén, ideértve a hitelesítési információk megfelelő kezelésével kapcsolatos tanácsadást a személyzet számára;

c) kezdetben, majd előre meghatározott időközönként, illetve a hitelesítő adatok veszélyeztetésének gyanúja esetén megkövetelik a hitelesítő adatok megváltoztatását;

d) előre meghatározott számú sikertelen bejelentkezési kísérlet után megkövetelik a hitelesítő adatok visszaállítását és a felhasználó letiltását;

e) előre meghatározott inaktív időtartam után lezárják az inaktivitási periódust; valamint

f) külön hitelesítő adatokat kérnek a különleges jogosultságú vagy adminisztratív fiókokhoz való hozzáféréshez.

11.6.3. Ha megvalósítható, az érintett szervezetek a legkorszerűbb hitelesítési módszereket alkalmazzák, a kapcsolódó értékelt kockázatnak és a hozzáféréssel elérni kívánt eszköz minősítésének megfelelően, valamint egyedi hitelesítési információkat használnak.

11.6.4. Az érintett szervezetek tervezett időközönként felülvizsgálják a hitelesítési eljárásokat és technológiákat.

11.7. *Többtényezős hitelesítés*

11.7.1. Az érintett szervezetek biztosítják, hogy a felhasználókat – ha indokolt – több hitelesítési tényező vagy folyamatos hitelesítési mechanizmus hitelesítse az érintett szervezetek hálózati és információs rendszereihez való hozzáférés érdekében, a hozzáféréssel elérni kívánt eszköz minősítésének megfelelően.

11.7.2. Az érintett szervezetek biztosítják, hogy a hitelesítés foka megfeleljen a hozzáféréssel elérni kívánt eszköz minősítésének.

12. **Eszközgazdálkodás (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének i) pontja)**

12.1. *Az eszközök minősítése*

12.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése i) pontjának alkalmazásában az érintett szervezetek a kívánatos védelmi szint megállapítása érdekében meghatározzák a hálózati és információs rendszereik hatókörébe tartozó valamennyi eszköz – így többek között az információk – minősítési szintjeit.

12.1.2. Az 12.1.1. pont alkalmazásában az érintett szervezetek:

a) megalkotják az eszközök minősítési szintjének rendszerét;

b) a bizalmas kezelésre, integritásra, hitelességre és rendelkezésre állásra vonatkozó követelmények alapján minden eszközhöz minősítési szintet rendelnek a kívánatos védelmi szintnek az eszközök érzékenysége, kritikus mivolta, kockázata és üzleti értéke alapján történő megállapítása érdekében;

c) az eszközökre vonatkozó rendelkezésreállási követelményeket összehangolják az üzletmenet-folytonossági és katasztrófa-helyreállítási terveikben meghatározott teljesítési és helyreállítási célkitűzésekkel.

12.1.3. Az érintett szervezetek rendszeres időközönként felülvizsgálják, és ha indokolt, frissítik a minősítési szinteket.

12.2. *Az eszközök kezelése*

12.2.1. Az érintett szervezetek hálózat- és információbiztonsági szabályzatukkal összhangban szabályzatot dolgoznak ki, hajtanak végre és alkalmaznak az eszközök – így többek között az információk – megfelelő kezelésére, és az eszközök megfelelő kezelésére vonatkozó szabályzatot megismertetik minden olyan személlyel, aki az eszközöket használja vagy kezeli.

12.2.2. A szabályzatnak:

a) le kell fednie az eszközök teljes életciklusát, ideértve a beszerzést, a használatot, a tárolást, a szállítást és az elidegenítést is;

b) rendelkezéseket kell tartalmaznia az eszközök biztonságos használatáról, biztonságos tárolásáról, biztonságos szállításáról, valamint helyrehozhatatlan törléséről és megsemmisítéséről;

c) elő kell írnia, hogy az átruházásnak biztonságos módon, az átruházandó eszköz típusának megfelelően kell megtörténnie.

12.2.3. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a szabályzatot.

12.3. *Az eltávolítható adathordozókra vonatkozó szabályzat*

12.3.1. Az érintett szervezetek az eltávolítható adathordozók kezelésére vonatkozó szabályzatot dolgoznak ki, hajtanak végre és alkalmaznak, és azt megismertetik az eltávolítható adathordozókat az érintett szervezetek telephelyein vagy más olyan helyszíneken kezelő alkalmazottaikkal és harmadik felekkel, ahol az eltávolítható adathordozók az érintett szervezetek hálózati és információs rendszereihez kapcsolódnak.

12.3.2. A szabályzatnak:

a) rendelkeznie kell az eltávolítható adathordozók csatlakoztatásának technikai tilalmáról, kivéve, ha használatuknak szervezeti oka van;

b) rendelkeznie kell az ilyen adathordozókról történő automatikus végrehajtás megakadályozásáról, valamint azoknak a rosszindulatú kódok tekintetében történő átvizsgálásáról az érintett szervezetek rendszereiben való felhasználást megelőzően;

c) intézkedéseket kell előírnia az adatokat tartalmazó hordozható tárolóeszközök ellenőrzésére és védelmére az adatátvitel és a tárolás során;

d) ha indokolt, intézkedéseket kell előírnia kriptográfiai technikák alkalmazására az eltávolítható adathordozókon tárolt adatok védelme érdekében.

12.3.3. Az érintett szervezetek tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a szabályzatot.

12.4. *Eszközleltár*

12.4.1. Az érintett szervezetek teljes körű, pontos, naprakész és következetes leltárt készítenek és vezetnek eszközeikről. Az eszközleltárban szereplő tételek változásait nyomon követhető módon rögzítik.

12.4.2. Az eszközleltár részletességének az érintett szervezetek igényeihez kell igazodnia. A leltárnak magában kell foglalnia a következőket:

a) a műveletek és szolgáltatások jegyzéke és leírása,

b) az érintett szervezetek működését és szolgáltatásait támogató hálózati és információs rendszerek és egyéb kapcsolódó eszközök jegyzéke.

12.4.3. Az érintett szervezetek rendszeresen felülvizsgálják és frissítik a leltárt és eszközeiket, és dokumentálják a változások előzményeit.

12.5. *Az eszközök leadása, visszaszolgáltatása vagy törlése a foglalkoztatás megszűnésekor*

Az érintett szervezetek olyan eljárásokat hoznak létre, hajtanak végre és alkalmaznak, amelyek biztosítják, hogy a személyzet által őrzött eszközöket a foglalkoztatás megszűnésekor leadják, visszaszolgáltassák vagy töröljék, valamint ezen eszközök leadása, visszaszolgáltatása és törlése dokumentálásra kerüljön. Amennyiben az eszközök leadása, visszaszolgáltatása vagy törlése nem lehetséges, az érintett szervezetek biztosítják, hogy az eszközökkel a továbbiakban ne lehessen hozzáférni az érintett szervezetek hálózati és információs rendszereihez, összhangban a 12.2.2. ponttal.

13. **Fizikai és környezeti biztonság (az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének c), e) és i) pontja)**

13.1. *Az ellátást biztosító közművek*

13.1.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése c) pontjának alkalmazásában az érintett szervezetek megelőzik a hálózati és információs rendszerek kiesését, károsodását vagy veszélyeztetését, illetve működésük megszakítását az ellátást biztosító közművek meghibásodása és zavara miatt.

13.1.2. E célból az érintett szervezetek, ha indokolt:

a) megvédik a létesítményeket a közművek – úgy mint a villamos energiával, távközléssel, vízzel, gázzal, szennyvízzel, szellőztetéssel, légkondicionálással összefüggő szolgáltatások – ellátási hiányosságai által okozott teljesítménykimaradásoktól és egyéb zavaroktól;

b) mérlegelik redundáns közüzemi szolgáltatások igénybevételét;

c) az adatokat szállító vagy hálózati és információs rendszereket ellátó villamosenergia- és távközlési közüzemi szolgáltatásokat megvédik a lehallgatással és a károkozással szemben;

d) figyelemmel kísérik a c) pontban említett közüzemi szolgáltatásokat, és jelentést tesznek az illetékes belső vagy külső személyzetnek a 13.2.2. b) pontban említett minimális és maximális ellenőrzési küszöbértékeken kívül eső, a közüzemi szolgáltatásokat befolyásoló eseményekről;

e) vészhelyzeti ellátásra vonatkozó szerződéseket kötnek a megfelelő szolgáltatókkal, például a vészhelyzeti áramellátáshoz szükséges üzemanyag tekintetében;

f) biztosítják a kínált szolgáltatás működtetéséhez szükséges hálózati és információs rendszerek folyamatos hatékonyságát, azokat figyelemmel kísérik, karbantartják és tesztelik, különös tekintettel a villamosenergia-ellátásra, a hőmérséklet- és páratartalom-szabályozásra, a távközlésre és az internetkapcsolatra.

13.1.3. Az érintett szervezetek rendszeres időközönként, illetve jelentős biztonsági eseményeket, a működést érintő nagyobb változásokat követően, vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a védelmi intézkedéseket.

13.2. *Védelem a fizikai és környezeti fenyegetésekkel szemben*

13.2.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése e) pontjának alkalmazásában az érintett szervezetek a 2.1. pont szerint elvégzett kockázatértékelés eredményei alapján megelőzik a fizikai és környezeti fenyegetésekből, például természeti katasztrófákból és egyéb szándékos vagy nem szándékos fenyegetésekből eredő eseményeket, vagy mérsékelik azok következményeit.

13.2.2. E célból az érintett szervezetek, ha indokolt:

a) védelmi intézkedéseket dolgoznak ki és hajtanak végre a fizikai és környezeti fenyegetésekkel szemben;

b) meghatározzák a fizikai és környezeti fenyegetésekre vonatkozó minimális és maximális ellenőrzési küszöbértékeket;

c) nyomon követik a környezeti paramétereket, és jelentést tesznek az illetékes belső vagy külső személyzetnek a b) pontban említett minimális és maximális ellenőrzési küszöbértékeken kívül eső eseményekről.

13.2.3. Az érintett szervezetek rendszeres időközönként, illetve jelentős biztonsági eseményeket, a működést érintő nagyobb változásokat követően, vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a fizikai és környezeti fenyegetésekkel szembeni védelmi intézkedéseket.

13.3. *Biztonsági övezet és a fizikaihozzáférés-ellenőrzés*

13.3.1. Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdése i) pontjának alkalmazásában az érintett szervezetek megelőzik és nyomon követik a hálózati és információs rendszereikhez való jogosulatlan fizikai hozzáférést, az azokban okozott károkat és beavatkozásokat.

13.3.2. E célból az érintett szervezetek:

a) a 2.1. pont szerint elvégzett kockázatértékelés alapján biztonsági övezeteket állapítanak meg és alkalmaznak azon területek védelme érdekében, ahol hálózati és információs rendszerek és egyéb kapcsolódó eszközök találhatók;

b) megfelelő belépési ellenőrzésekkel és hozzáférési pontok révén gondoskodnak az a) pontban említett területek védelméről;

c) tervet készítenek és gondoskodnak az irodák, helyiségek és létesítmények fizikai biztonságáról;

d) folyamatosan ellenőrzik biztonsági övezeteiket a jogosulatlan fizikai hozzáférés tekintetében.

13.3.3. Az érintett szervezetek rendszeres időközönként, illetve jelentős biztonsági eseményeket, a működést érintő nagyobb változásokat követően, vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a fizikaihozzáférés-ellenőrzési intézkedéseket.