

Műszaki követelmények IBF támogatás és sérülékenység vizsgálat szolgáltatás vonatkozásában

1. Előzmények

Az Ajánlatkérő számára kiemelten fontos elektronikus információs rendszereink biztonságos működése, illetve a releváns kiberbiztonsági jogszabályoknak történő megfelelés, ezért támogatást kívánunk igénybe venni azok tervezésében, üzemeltetésében és folyamatos ellenőrzésében. Feladataink közé tartozik az információbiztonsági szabályozások felülvizsgálata és továbbfejlesztése, a beszállítókkal kötött szerződések biztonsági szempontú áttekintése, valamint rendszeres sérülékenységvizsgálatok elvégzése. A közeljövőben meghatározó feladatunk a NIS2 irányelv és a kapcsolódó hazai szabályozásoknak való megfelelésre való felkészülés

2. A szolgáltatás tartalma

2.1.Sérülékenység vizsgálat

a) Vizsgálat terjedelme

Az Ajánlatkérő érintett informatikai infrastruktúrája, igény szerint belső és külső vizsgálat (szerverek, hálózati eszközök, végpontok, alkalmazások). Konfigurációs hibák, elavult komponensek és engedélykiosztási problémák feltárása.

b) Minőségi követelmények

Nemzetközi szabványoknak és hazai jogszabályoknak megfelelő vizsgálati módszertanok alkalmazása, korszerű, licencelt és naprakész automatizált eszközök használata, illetve szükség esetén manuális ellenőrzések elvégzése a téves riasztások kiszűrésére és kritikus hibák igazolására.

c) Jelentéskészítés

Részletes, magyar nyelvű vizsgálati jelentés, amely tartalmazza a feltárt sérülékenységek listáját és azok kockázati besorolását, a sérülékenységek pontos helyét és reprodukálásának módját, a sérülékenységek pontos helyét és reprodukálásának módját, illetve összefoglalót a legfontosabb megállapításokkal.

d) Adatkezelési és biztonsági feltételek

A vizsgálat kizárólag a szervezet előzetes engedélye és jóváhagyott időablaka alapján végezhető. A vállalkozó köteles biztosítani az adatok bizalmas kezelését. A vizsgálat során megszerzett információkat a szolgáltató nem oszthatja meg harmadik féllel. A vizsgálat nem okozhat szolgáltatáskimaradást vagy teljesítményromlást.

e) Konzultáció és támogatás

A vizsgálat eredményeinek részletes áttekintése szakmai egyeztetésen. Igény szerint utóvizsgálat annak ellenőrzésére, hogy a javítások megtörténtek-e.

2.2.Kockázatmenedzsment keretrendszer kialakítása

A 7/2024. (VI. 24.) MK rendeletben előírt kockázatmenedzsment keretrendszer kialakítása és bevezetése az Ajánlatkérő információs rendszereire vonatkozóan.

A szolgáltatás tartalma:

- Kockázatmenedzsment stratégia kialakítása
- Szerepkörök és felelősségi körök meghatározása
- Védelmi intézkedések megfelelőségének felmérése és dokumentálása
- Feltételezések, prioritások és kompromisszumok rendszerezése
- Rendszeres felülvizsgálati mechanizmus kialakítása
- Monitoring- és riportolási folyamatok kialakítása
- Védelmi intézkedések rendszeres értékelése
- Dokumentáció karbantartása és naprakészen tartása

2.3.IBF támogatás

Ajánlatkérő elektronikus információs rendszereinek biztonsági tervezésének, működtetésének és ellenőrzésének támogatása az információbiztonsági szabályozók felülvizsgálata, továbbfejlesztése, valamint a releváns szállítói szerződések biztonsági szempontú véleményezése. A következő időszak egyik fő feladata, várhatóan a NIS 2 rendelet, illetve a kapcsolódó hazai jogszabályoknak történő megfelelésre való felkészülés lesz.

Kategória	Feladat	Ajánlattevő által elvégzett feladat	Ajánlatkérő feladata
Információbiztonsági irányítási rendszer	Állapotfelmérés	X	
	Szóbeli, írásbeli tájékoztatás	X	
	Kockázatok feltárása	X	
	Javaslattétel a kockázatok elhárítására	X	
	Konkrét intézkedések a kockázatkezelésre		X
Szervezet elektronikus információs rendszerei	Állapotfelmérés (jogszabályi megfeleltetés)	X	
	Szóbeli, írásbeli tájékoztatás	X	
	Javaslattétel a jogszabályi informatikai megfelelésre	X	
	Konkrét intézkedések megtétele		X
	Biztonsági osztályba sorolás előkészítése		X
	A szervezet biztonsági szintbe sorolására javaslat		X
Informatikai biztonsági szabályzat	Előkészítés	X	
	Frissítés, naprakészen tartása	X	
	Meglévő szabályozók felülvizsgálata	X	
	Meglévő szabályozók továbbfejlesztése	X	
	Jóváhagyás		X
Elektronikus információs rendszerek dokumentumai	Biztonsági szempontból véleményezés	X	
	Tervezési javaslattétel	X	
	Fejlesztési javaslattétel	X	
	Jogszabályi informatikai megfelelés támogatása	X	
	Üzemeltetési javaslattétel	X	
	Konkrét intézkedések megtétele		X

Biztonsági audit	Auditra való felkészülés támogatása	X	
	Audit eredményeinek kiértékelése	X	
	Javaslattevél az auditot követően	X	
	Konkrét intézkedések megtétele		X
Hatósági kapcsolat	Kapcsolattartás a hatósággal		X
	Kapcsolattartás a kormányzati eseménykezelő központtal		X
	Hatósági válaszlevelek előkészítése		X
	Biztonsági incidensekről hatósági tájékoztatása munkanapokon		X
	Előzetes tájékoztatási formanyomtatvány előkészítése		X

3. Egyéb elvárások

- a) A szolgáltatás időtartama: 12 hónap. A teljes futamidő alatt a havi díj rögzített, annak díja nem változhat.
- b) Fizetési gyakoriság: havonta.
- c) A Havidíjban foglalt óraszámok:
 - Távoli munkavégzés és eseti konzultáció telefonon vagy online: 20 óra
 - Helyszíni egyeztetés: negyedévente egy alkalom
 - A havi keret fel nem használt munkaórái a következő hónapra átvihetők és ott felhasználhatók.
- d) Lehetőség a havi óraszámom felüli helyszíni és távoli munkavégzésre is külön díjazás ellenében, de maximum 120 óra/év mértékben.
- e) Rendelkezésre állás munkanapokon 5x8 órában.