Съвет на
Европейския съюз

Брюксел, 22 март 2022 г.
(OR. en)

7474/22
ADD 1

Междуинституционално досие:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

ПРЕДЛОЖЕНИЕ

От:	Генералния секретар на Европейската комисия, подписано от г-жа MARTINE DEPREZ, директор
Дата на получаване:	22 март 2022 г.
До:	Г-н Jeppe TRANHOLM-MIKKELSEN, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2022) 122 final - Annexes 1 to 2
Относно:	ПРИЛОЖЕНИЯ към Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза

Приложено се изпраща на делегациите документ COM(2022) 122 final - Annexes 1 to 2.

Приложение: COM(2022) 122 final - Annexes 1 to 2

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 22.3.2022 г.
COM(2022) 122 final

ANNEXES 1 to 2

ПРИЛОЖЕНИЯ

към

Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ПРИЛОЖЕНИЕ I

Следните области трябва да бъдат обхванати в базовия набор от мерки за киберсигурност:

1) политика в областта на киберсигурността, включително цели и приоритети за сигурността на мрежите и информационните системи, по-специално по отношение на използването на облачни изчислителни услуги (по смисъла на член 4, параграф 19 от Директива [предложение за МИС 2]), и технически договорености, позволяващи работа от разстояние;

2) организация на киберсигурността, включително определяне на ролите и отговорностите;

3) управление на активите, включително инвентарен опис на ИТ активите и картографиране на ИТ мрежата;

4) контрол на достъпа;

5) сигурност на операциите;

6) сигурност на комуникациите;

7) придобиване, разработка и поддръжка на системи;

8) отношения с доставчиците;

9) управление на инциденти, включително подходи за подобряване на готовността, реагирането и възстановяването от инциденти и сътрудничеството със CERT-EU, като например осъществяване на мониторинг на сигурността и водене на регистри;

10) управление на непрекъснатостта на дейностите и управление на кризи; както и

11) образование, повишаване на осведомеността и програми за обучение в областта на киберсигурността.

ПРИЛОЖЕНИЕ II

Институциите, органите и агенциите на Съюза разглеждат най-малко следните специфични мерки за киберсигурност при реализирането на базовия набор от мерки за киберсигурност и в своите планове за киберсигурност в съответствие с документите с насоки и препоръките на МСК:

1) конкретни стъпки за преминаване към архитектура с нулево доверие (т.е. модел за сигурност, набор от правила за проектиране на системи и координирана стратегия за киберсигурност и управление на системи, основаваща се на разбирането, че заплахи съществуват както вътре, така и извън традиционните граници на мрежите);

2) приемане на многофакторната автентификация като норма в мрежите и информационните системи;

3) установяване на сигурността на веригите за доставка на софтуер чрез критерии за сигурно разработване и оценка на софтуера;

4) подобряване на правилата за възлагане на обществени поръчки, за да се улесни постигането на високо общо ниво на киберсигурност чрез:

   а) премахване на договорните пречки, които ограничават доставчиците на ИТ услуги да споделят информация със CERT-EU относно инциденти, уязвимости и киберзаплахи;

   б) договорно задължение за докладване на инциденти, уязвимости и киберзаплахи, както и за въвеждане на подходящи механизми за реакция и мониторинг на инцидентите.