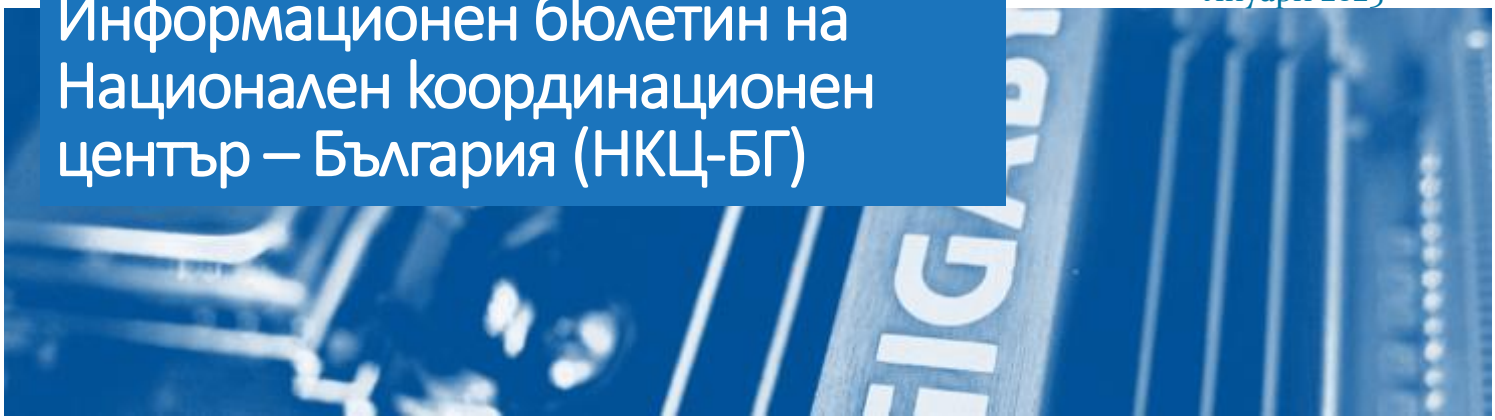
Министерство на електронното управление

Съфинансирано от Европейския съюз

Информационен бюлетин на Национален координационен център – България (НКЦ-БГ)

Януари 2025



DORA (DIGITAL OPERATIONAL RESILIENCE ACT) – ЕВРОПЕЙСКИЯТ РЕГЛАМЕНТ ЗА ЦИФРОВАТА ОПЕРАТИВНА УСТОЙЧИВОСТ

Какво представлява DORA?

В света на цифровата сигурност регулациите се развиват с бързи темпове, а адаптацията към тях не е просто формалност, а стратегическа необходимост. Един от най-значимите регулаторни актове в сферата на финансовата сигурност е DORA (Digital Operational Resilience Act) – Европейският регламент за цифровата оперативна устойчивост. Той налага строги изисквания към финансовите институции и доставчиците на ИТ

Той въвежда задължителни изисквания за управление на ИТ рисковете, надзор върху доставчиците на услуги, както и механизми за тестване на устойчивостта срещу кибератаки.

Влиянието на регулацията не се ограничава само до банки и застрахователни компании. Тя засяга и финтех компании, инвестиционни фондове, кредитни посредници, платежни оператори и дори технологичните доставчици на тези организации. Ако вашият бизнес попада в обхвата на DORA, пропускането на изискванията може да доведе до глоби, регулаторни санкции или дори отнемане на лицензи.

ОСНОВНИ ИЗИСКВАНИЯ НА МИС2

Директивата налага редица задължения на засегнатите субекти, включително:

- Управление на риска: Организациите трябва да приемат мерки за управление на риска, свързан с киберсигурността, включително оценка на рисковете, внедряване на подходящи технически и организационни мерки и редовен мониторинг.

-Докладване на инциденти: Значителни инциденти, които засягат предоставянето на услуги, трябва да бъдат докладвани на компетентните органи в



услуги, с цел укрепване на кибер устойчивостта в сектора. DORA е част от по-широката стратегия на ЕС за повишаване на устойчивостта на финансовите институции срещу киберзаплахи.

DORA не е просто „кутия за отбелязване“. Регулацията изисква постоянно усъвършенстване, мониторинг и реакция на нови заплахи. Попълването на въпросника ще ви даде отправна точка, но следващата стъпка е разработването и внедряването на цялостна стратегия за киберустойчивост.

Независимо дали започвате или вече сте в процес на привеждане в съответствие, този инструмент е ключът към навременни и информирани действия. Защото в ерата на цифровите финанси оцеляването и успехът се определят от устойчивостта срещу рискове, а тя започва със знанието.





определени срокове.

- Сигурност на веригата на доставки: Организациите трябва да управляват рисковете, свързани с техните доставчици и партньори, като гарантират, че и те спазват изискванията за киберсигурност.

-Транспониране в българското законодателство

В България процесът на транспониране на МИС2 е в ход. На 4 юли 2024 г. Министерството на електронното управление внесе законопроект за изменение и допълнение на Закона за киберсигурност, с който се транспонира директивата.

С навлизането на МИС2 киберсигурността става не само технически, но и стратегически приоритет за организациите. Навременното адаптиране към новите изисквания ще гарантира не само съответствие със закона, но и повишена устойчивост срещу киберзаплахи.



ДИРЕКТИВА (ЕС) 2022/2555 – МИС 2

Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година представя мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (ОВ, L 333, 27.12.2022г.), наричана по-нататък „Директивата МИС 2".

Една от основните цели на Директива (ЕС) 2022/2555 е осигуряването на високи гаранции и възможности за по-добра устойчивост на киберпространството и по-ефективни мерки за противодействие на кибератаките, особено по отношение на основните икономически субекти и държавните органи. В този смисъл новите регулации целят гарантиране на справедливо третиране на субектите, повишаване на тяхната информираност и осигуряване на надежден и ефективен надзор за спазване на правата и законните им интереси.

РАЗШИРЕН ОБХВАТ НА МИС2

МИС2 значително разширява обхвата на секторите и организациите, които попадат под нейните изисквания. Докато МИС1 обхващаше седем сектора, включително енергетика, транспорт и здравеопазване, МИС2 добавя нови сектори, базирани на тяхната критичност за икономиката и обществото. Сред тях са:

- Пощенски и куриерски услуги

- Управление на отпадъци

- Производство и дистрибуция на химикали

- Производство на храни

- Производство на медицински изделия

КРИТЕРИИ ЗА ОПРЕДЕЛЯНЕ НА ЗАСЕГНАТИТЕ СУБЕКТИ

МИС2 въвежда ясни критерии за определяне на засегнатите субекти. Всички средни и големи предприятия в посочените сектори попадат в обхвата на директивата. Средни предприятия са тези с персонал между 50 и 249 служители и годишен оборот между 10 и 50 милиона евро, докато големите предприятия имат над 250 служители и оборот над 50 милиона евро. Това означава, че дори организации, които не се считат за критична инфраструктура, но отговарят на тези критерии, ще бъдат засегнати.



ОРГАНИЗАЦИИТЕ, ПОПАДАЩИ В ОБХВАТА НА МИС2, ТРЯБВА ДА ПРЕДПРИЕМАТ СЛЕДНИТЕ СТЪПКИ:

-Оценка на съответствието, т.е. да определят дали попадат в обхвата на директивата въз основа на сектора и размера си.

- Оценка на риска - да извършат подробен анализ на текущите си практики за киберсигурност и да идентифицират пропуските спрямо изискванията на МИС2.

- Разработване на план за действие – да създадат и внедрят план за постигане на съответствие, включително обучение на персонала, внедряване на технически мерки и установяване на процедури за докладване на инциденти.







Министерство на електронното управление

ул. „Ген. Гурко“ № 6

Гр. София 1000

Ел. поща: bnccc@egov.government.bg

Ел. адрес: https://ncc.egov.bg/