DORA – DIGITAL OPERATIONAL RESILIENCE ACT

DORA – ЗАКОН ЗА ДИГИТАЛНА ОПЕРАТИВНА ОТПОРНОСТ

Општо

Законот за дигитална оперативна отпорност (DORA) конкретно се фокусира на финансиските субјекти, со цел да ја зголеми нивната отпорност на нарушувања поврзани со ИКТ. Законот ги наведува барањата за широк спектар на финансиски субјекти, за воспоставување на сеопфатни дигитални рамки за оперативна отпорност.

- Финансиски субјекти: Регулативата DORA се применува на банки, осигурителни компании, инвестициски друштва, па дури и даватели на услуги за крипто-валути и трети лица на ИКТ провајдери.
- Мерки за оперативна отпорност: Вклучува управување со ИКТ (Информациска и Комуникациска Технологија) ризик, известување за инциденти, дигитално тестирање на оперативни отпорности и управување со ризик од трета страна.
- Зајакнување на финансискиот сектор: Осигурува дека финансискиот сектор може да издржи и брзо да закрепне од дигитални нарушувања, зачувувајќи го интегритетот и стабилноста на финансиските пазари во ЕУ.

Законот за дигитална оперативна отпорност (DORA) е значаен дел од законодавството во рамките на Европската Унија. За разлика од NIS 2, тој е специјално направен за да ја зајакне отпорноста на финансискиот сектор на ИКТ ризиците.

Еден од најголемите наративи на DORA е да ја препознае важноста на дигиталната инфраструктура во финансиската индустрија. Значи, има создадено безбедна рамка за да се осигура дека банките, финансиските институции, па дури и новите финансиски субјекти, како што се давателите на услуги за крипто-валути, можат да издржат, да реагираат и закрепнат од широкиот спектар на дигитални нарушувања.

Во својата основа, DORA наложува примена на ригорозни ИКТ способности за управување со ризик. Тоа вклучува воспоставување на отпорна дигитална оперативна инфраструктура, темелно тестирање на дигиталната оперативна отпорност и детални механизми за известување за инциденти. Овој пристап не само што има цел да го ублажи влијанието на потенцијалните инциденти поврзани со ИКТ, туку и ја зголемува вкупната стабилност и интегритет на финансиските пазари во ЕУ.

Еден од клучните аспекти на DORA е нејзиниот инклузивен опсег кој се однесува на широк спектар на финансиски субјекти. Оваа инклузивност осигурува дека DORA се однесува на

дигиталната оперативна отпорност на финансискиот систем како целина, а не во изолирани сегменти.

Покрај тоа, DORA е значајна во однос на важноста на управувањето со ризик од трета страна. Признава дека многу финансиски субјекти се потпираат на надворешни даватели на услуги за критични ИКТ услуги. Со охрабрување на организациите да спроведуваат длабинска анализа и договорни аранжмани, целта на DORA е да ги прошири своите стандарди за издржливост низ синџирот на снабдување.

За кого се однесува DORA?

- банки и останати финансиски институции;
- институции за платен промет;
- даватели на информативни услуги за платежни сметки;
- институции за дигитални пари;
- инвестициски компании;
- даватели на услуги за крипто-валути и издавачи на токени поврзани со дигитални средства;
- централни депозитари за хартии од вредност;
- централни договорни страни;
- места на трансакции;
- складишта за трансакции;
- управители на алтернативни инвестициски фондови;
- друштва за управување;
- даватели на услуги за известување и обработка на податоци;
- друштва за осигурување и реосигурување;
- посредници во осигурување, посредници во реосигурување и помошни посредници во осигурување;
- институции за професионално пензиско осигурување;
- агенции за оценување на кредитен рејтинг;
- администратори на критични мерила;
- даватели на услуги за групно финансирање;
- складишта за хартии од вредност;
- даватели на услуги од трета страна.

Барања на DORA

DORA има 5 главни барања (столба), и тоа се:

1) Управување со ризик од информатичка и комуникациска технологија (ИКТ).
DORA бара од повисокото раководство да преземе одговорност за управување со ризикот од ИКТ, да ги идентификува критичните функции и да воспостави рамка за управување со ризик заснована на меѓународни стандарди. Оваа рамка за управување мора да се ревидира секоја година.

2) Пријавување на инциденти во информатичка и комуникациска технологија
DORA бара од финансиските субјекти да уредуваат и пренесуваат извештаи за инциденти во информатичката и комуникациската технологија. Регулативата DORA има за цел да го усогласи откривањето на инциденти и нивно известување низ цела Европа.

3) Тестови за дигитални оперативни отпорности

Финансиските институции треба да спроведуваат тестови за отпорност и ранливост на дигиталната инфраструктура најмалку еднаш годишно, спроведени од независни страни. Овие тестови се дизајнирани да ја проценат способноста на целните компании да управуваат со инцидентите и да ги идентификуваат слабостите на системот, користејќи пристап заснован на ризик. Пред да се имплементираат нови услуги или да се надградат веќе постоечките кои ги поддржуваат нивните критични функции, потребни се проценки на ранливост за да се обезбеди оперативна отпорност на IT системите.

4) Управување со ризик од трета страна

DORA ги проширува обврските во однос на аутсорсингот на ИКТ услугите на добавувачи од трети страни, барајќи од финансиските субјекти да управуваат со ризиците поврзани со овие добавувачи. Тие мора да ги проценат договорните ризици, да ги раскинат договорите со добавувачите кои претставуваат ризици за сајбер безбедноста и да изработа годишен извештај за договорот.

5) Споделување на информации и податоци

DORA ги дефинира клучните принципи за управување со ризиците поврзани со добавувачите на ИКТ. DORA ги охрабрува финансиските институции да споделуваат информации за сајбер заканите, за да ги намалат ризиците поврзани со ИКТ. Регулативата ги овластува финансиските субјекти да воспоставуваат договори за размена на информации, истовремено гарантирајќи ја заштитата на личните податоци.

DORA започнува да се применува од 17 Јануари 2025 година.

Добри основи:

ISO/IEC 27001:2022; ISO/IEC 27002:2022; ISO/IEC 27701:2019; ISO/IEC 27005:2022; ISO/IEC 27032:2023; ISO/IEC 27035:2023; GDPR; CER – Critical Entities Resilience Directive

NIS 2 – NETWORK AND INFORMATION SECURITY DIRECTIVE

NIS 2 – ДИРЕКТИВА ЗА БЕЗБЕДНОСТ НА МРЕЖНИ И ИНФОРМАТИЧКИ СИСТЕМИ

Општо

„Директивата NIS 2" или едноставно „NIS 2" е директива на Европската Унија која ги специфицира барањата за сајбер безбедност што мора да ги имплементираат компаниите од ЕУ кои се сметаат за критична инфраструктура. Нејзиното целосно име е "Директива (ЕУ) 2022/2555 на Европскиот парламент на мерки за високо заедничко ниво на сајбер безбедност низ Унијата". NIS 2 е објавена на 14 Декември 2022 година.

Бидејќи NIS 2 е директива, тоа значи дека секоја земја во Европската Унија ќе ги дефинира своите закони за сајбер безбедност врз основа на NIS 2, додека NIS 2 го одредува минималното ниво на сајбер безбедност што треба да се постигне. Во пракса, тоа значи дека компаниите во едни земји ќе мора да се придржуваат до минимумот утврден во NIS 2, а во други ќе мора да се придржуваат до построгите барања за сајбер безбедност утврдени во локалните закони.

Директивата NIS 2 може да стане за сајбер безбедноста она што GDPR стана за приватноста – светски стандард што другите земји го користат како најдобра практика за нивното

законодавство. NIS 2 стапува на сила на 18 Октомври 2024 година. Ова е и крајниот рок за земјите од Европската Унија да ги дефинираат сопствените закони и прописи врз основа на NIS 2.

На кого се однесува NIS 2?

Постојат 3 критериуми што дефинираат кои организации (NIS 2 ги нарекува "значајни ентитети" и "важни ентитети") мора да се усогласат со NIS 2:

1) Локација – ако даваат услуги или вршат активности во било која земја на Европската Унија (без разлика дали се наоѓаат во ЕУ или не);

2) Големина – ако имаат повеќе од 50 вработени и имаат приход повеќе од 10 милиони евра;

3) Индустрија – ако работат во некој од следните сектори:

- Сектори со висока критичност:
  - енергија (електрична енергија, централно греење и ладење, нафта, гас и водовод);
  - транспорт (воздушен, железнички, воден и патен);
  - банкарство;
  - инфраструктура на финансискиот пазар;
  - здравје, вклучително и производство на фармацевтски производи и вакцини;
  - вода за пиење;
  - отпадни води;
  - дигитална инфраструктура (интернет хабови, даватели на DNS услуги, регистри со имиња на главни домени, даватели на услуги за cloud, даватели на услуги за дата центри, мрежи за испорака на содржина, даватели на услуги за дигитални сертификати, даватели на јавни електронски комуникациски мрежи и јавно достапни електронски комуникациски услуги);
  - управување со ИКТ услуги (даватели на услуги со кои се управува и даватели на управувани безбедносни услуги) и јавна администрација;
- Останати клучни сектори:
  - поштенски и курирски услуги;
  - управување со отпад;
  - хемикалии;
  - храна;
  - производство на медицински производи, компјутери и електроника, машини и опрема, моторни возила, приколки и полуприколки и друга транспортна опрема;
  - дигитални провајдери (интернет пазар, интернет пребарувачи и платформи за услуги за социјални мрежи) и истражувачки организации;

Барања на NIS 2

Технички мерки:

- Управување со ризици: Организациите мора да преземат мерки за минимизирање на сајбер ризиците, вклучувајќи управување со инциденти, зајакнување на безбедноста на

синџирот за снабдување, подобрување на безбедноста на мрежата, подобра контрола на пристапот и шифрирање.
- Корпоративна одговорност: NIS 2 бара од корпоративното раководство да ги надгледува, одобрува и обучува мерките за сајбер безбедност и да одговори на сајбер ризиците.
- Обврски за известување: Критичните субјекти мора да имаат воспоставено процеси за брзо известување за безбедносни инциденти кои значително влијаат на нивното давање или примање на услуги.
- Деловен континуитет: Организациите мора да планираат како ќе обезбедат деловен континуитет во случај на големи сајбер инциденти. Овој план треба да вклучи размислувања за обновување на системот, процедури за итни случаи и формирање на тим за реагирање во случај на криза.

Основни безбедносни мерки:
Покрај овие општи области на барања, NIS 2 наложува суштинските и важните ентитети да имплементираат основни безбедносни мерки за справување со специфични форми на веројатни сајбер закани.
Тоа вклучува:

- Проценка на ризик и безбедносни политики за информациски системи;
- Политики и процедури за проценка на ефективноста на безбедносните мерки;
- Политики и процедури за употреба на криптографија и, кога е релевантно, шифрирање;
- План за справување со безбедносни инциденти;
- Безбедност на набавка, развој и системско работење;
- Обука за сајбер безбедност и практика за основна компјутерска хигиена;
- Безбедносни процедури за вработените кои имаат пристап до осетливи и важни податоци;
- План за управување со деловните операции за време и по безбедносен инцидент;
- Употреба на повеќефакторска автентикација, решенија за континуирана автентикација, шифрирање на глас, видео и текст, и шифрирани интерни комуникации во итни случаи, кога тоа е прифатливо;
- Безбедност на синџирите на снабдување и односите помеѓу компанијата и директните добавувачи;

Добри основи:
ISO/IEC 27001:2022; ISO/IEC 27002:2022; ISO/IEC 27701:2019; ISO/IEC 27005:2022; ISO/IEC 27032:2023; ISO/IEC 27035:2023; GDPR; CER – Critical Entities Resilience Directive; ISO/IEC 27036-2:2023

Неисполнување на барањата на DORA и NIS 2

Неисполнување на барањата на DORA и NIS 2 може да доведе до сериозни последици. Ова вклучува законски мерки и високи касни за непочитување.