Průzkum připravenosti českých společností na příchod směrnice NIS2

Únor 2024

NIS2: Nejen legislativa, ale cesta k digitální svobodě a prosperitě. V dnešní digitální éře je právě bezpečnost klíčová pro prosperitu a konkurenceschopnost firem.

EY
Building a better working world

Současný stav legislativy

Evropský parlament na svém jednání dne 10. listopadu 2022 a Rada Evropské unie na jednání dne 28. listopadu 2022 přijaly finální znění směrnice NIS2. Transpoziční lhůta (tj. lhůta pro začlenění směrnice do české legislativy) je zhruba 22 měsíců od jejího schválení, tedy přibližně do října roku 2024. Transpozice do české legislativy proběhne formou novelizace stávajících zákonů a prováděcích předpisů. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) publikoval dne 26. ledna 2023 návrh aktualizovaného znění Zákona o kybernetické bezpečnosti a souvisejících vyhlášek pro připomínkování odborné veřejnosti, a následně 26. ledna 2024 předložil Legislativní radě vlády poslední novelizovanou verzi legislativy.

Zcela konkrétní datum platnosti všech novelizovaných povinností pro regulované subjekty není prozatím známo, nicméně ze zkušenosti můžeme očekávat zhruba roční lhůtu, tedy konec roku 2025. Do této doby budou muset regulované subjekty naplnit všechny požadavky zákona a příslušných prováděcích předpisů.

Velká část společností, zejména ty, jež spadají pod stávající regulaci zákona o kybernetické bezpečnosti, značnou část opatření již naplňují. Je zde ale mnoho subjektů, pro které měly investice do kybernetické bezpečnosti dlouhodobě nízkou prioritu a tyto společnosti budou k zajištění souladu s požadavky NIS2 muset vynaložit nejen úsilí, ale také nemalé finanční prostředky.

Návrh novelizace zavádí dva odlišné režimy úrovní povinností, avšak samotná opatření stanovená stávající legislativou se významně nezpřísňují. Zásadní novinkou je podstatné zvýšení sankcí, je ale potřeba zmínit i další změny, které pozorujeme v souvislosti s transpozicí nové směrnice NIS2. Jedná se o sebeurčení, kontrolní hlášení či prokazování kybernetické odolnosti regulovaného subjektu.

O průzkumu

Úvod průzkumu

Společnost EY Česká republika v souvislosti se zaváděním směrnice NIS2 uskutečnila průzkum připravenosti českých společností na tuto směrnici. Průzkum probíhal od 12. prosince 2023 do 19. ledna 2024 formou dotazníkového šetření. Tohoto průzkumu se účastnili zástupci desítek společností z 22 různých odvětví (státní správa, zdravotnictví, ICT služby a další).

Průzkum jsme využili k prvotnímu orientačnímu posouzení připravenosti a informovanosti firem ohledně nové regulace NIS2. Cílem průzkumu bylo získat ucelený přehled o problematice spojené s NIS2 a shromáždit základní data o:

- Aktuálním stavu implementace NIS2 v českých firmách.
- Vnímání regulace ze strany firem.
- Úrovni informovanosti o regulaci.
- Očekáváních a obavách firem v souvislosti s NIS2.

Vyhodnocení průzkumu

Jelikož se jedná o pilotní průzkum tématu, jemuž nebyla doposud věnována přílišná pozornost, mají naše prvotní závěry spíše indikativní charakter, problematickým a nejasným oblastem se plánujeme ještě dále věnovat. Ale již nyní můžeme říct, že:

2 %

Firem jsou v současnosti plně v souladu s NIS2

Znepokojivý trend v oblasti informovanosti

Téměř polovina nově regulovaných společností nemá dostatečné povědomí o problematice NIS2

NIS2: Povinnost, o které management neví

Z výsledků vyplývá znepokojivé zjištění – nízká úroveň povědomí o NIS2 mezi společnostmi, které spadají do její působnosti. NIS2 je důležitá legislativa, která má za cíl posílit kybernetickou bezpečnost v klíčových sektorech ekonomiky. Nedostatečná informovanost o NIS2 může vést k tomu, že se firmy nebudou adekvátně připravovat na splnění jejích požadavků, čímž se vystavují riziku sankcí.

Skutečnost, že čtvrtina všech respondentů nemá dostatečné povědomí o NIS2, je znepokojivá. Zhruba polovina respondentů, jenž uvedli, že nejsou dostatečně informováni, zastává vrcholné řídící pozice, nebo jsou členy představenstva. Nedostatečná angažovanost managementu v oblasti kybernetické bezpečnosti může mít vážné důsledky, protože vedení společnosti zajišťuje klíčovou roli v řízení kybernetické bezpečnosti.

26 %

všech respondentů nemá dostatečné povědomí o NIS2

Vedení společnosti

Kybernetická bezpečnost je pro firmy klíčová a **právě vedení společnosti dle NIS2 nese přímou zodpovědnost za její zajištění.** Nedostatečné povědomí vrcholového managementu o NIS2 může vést k ignorování problematiky kybernetické bezpečnosti a v konečném důsledku k nepřijetí adekvátních kroků pro splnění požadavků NIS2 a vystavení se sankcím ze strany regulátora.

Pro zlepšení povědomí managementu o NIS2 a kybernetické bezpečnosti je důležité:

Nedostatek odborníků – začátek doby automatizace a sdílených služeb

Více jak polovina všech respondentů (52 %) průzkumu uvedlo, že největší výzvy spatřuje v nedostatečných personálních kapacitách a ve výši nákladů spojených s implementací požadavků směrnice NIS2.

V souvislosti s počtem nově regulovaných subjektů, kterých se jen v ČR odhaduje na více než 6 000, očekáváme, že ve spojitosti s dalšími regulacemi z balíčku kybernetické odolnosti EU nastane na českém trhu ještě větší nedostatek odborníků v oblasti kybernetické bezpečnosti. Přístup a myšlení společností se bude muset, dle našeho názoru, v souvislosti se zaváděním NIS2 radikálně změnit, a to zejména u menších subjektů.

Řešení se nám však nabízí: v dnešní době sdílení, kdy je běžné si pronajímat městské automobily či kola, nabízí i oblast kybernetické bezpečnosti obdobnou alternativu. Společnosti, které nemají dostatečné personální a technické kapacity, mohou využít sdílených služeb a odborníky si na základě platných dohod nasdílejí.

Druhou cestou je automatizace, umělá inteligence a strojové učení. Neustále se zvyšující počet informačních systémů produkuje narůstající množství dat, což ve spojitosti s nedostatkem zaměstnanců způsobuje, že schopnost společností analyzovat a vyhodnocovat relevantní data je stále nižší. Právě proto je nutné se orientovat na relevantní hrozby a automatizované testování kybernetické odolnosti vůči nim.

Včasná příprava ušetří čas i peníze

Včasná příprava je klíčová pro naplnění požadavků novelizované regulace kybernetické bezpečnosti. Jak jsme uvedli, nová regulace kybernetické bezpečnosti NIS2 se blíží a s ní i termín pro dosažení souladu. Jaká je ale aktuální situace mezi českými firmami? Z našeho průzkumu vyplývá:

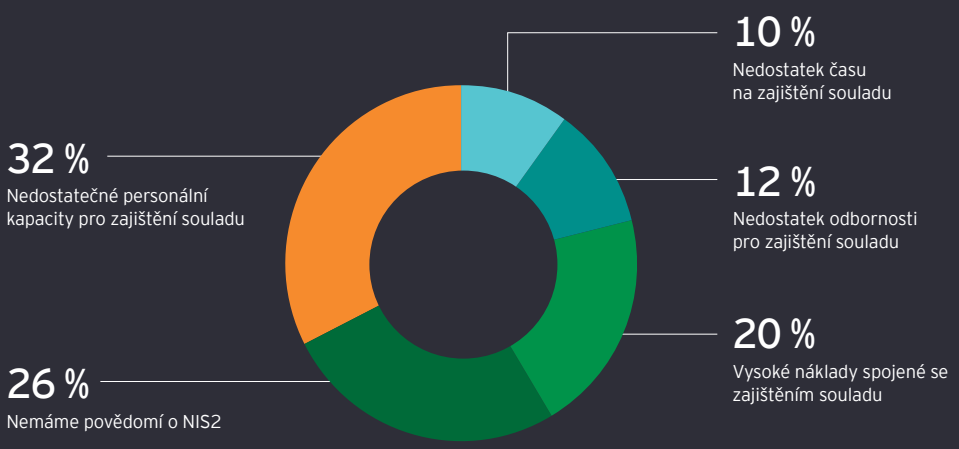
67 %
Firem chce být v souladu s NIS2 do konce roku 2024. To je pozitivní zpráva, která ukazuje, že firmy si uvědomují důležitost kybernetické bezpečnosti

52 %
Firem zatím nepodniklo žádné kroky k dosažení souladu s NIS2 To je znepokojivé, protože implementace potřebných opatření může být časově náročná

31 %
Firem plánuje splnit požadavky NIS2 až v roce 2025 nebo později. To představuje značné riziko, protože zpoždění může vést k pokutám a narušení provozu

2 %
Firem jsou v současnosti plně v souladu s NIS2

Největší výzvy



Změny v legislativě NIS2 stále probíhají, byť pomalejším tempem. I když se finální podoba návrhu legislativy ještě může mírně upravit, nebudou tyto změny natolik významné, aby ovlivnily již implementovaná opatření. Implementace některých opatření může být také časově náročná.
Průzkum mezi firmami v České republice ukázal, že pouze 2% firem se domnívá, že jsou plně v souladu s požadavky NIS2. To představuje značné riziko, protože kybernetické útoky se stávají stále sofistikovanějšími a firmy, které nebudou adekvátně chráněny, se vystavují riziku ztráty dat, narušení provozu, finančním škodám a reputačnímu dopadu.
Firmy, které dlouhodobě podceňovaly investice do kybernetické bezpečnosti, budou muset investovat do nových technologií a procesů. Nedostatečná ochrana před kybernetickými hrozbami představuje vážné riziko a implementace požadavků NIS2 by se tak pro ně měla stát prioritou.

Co dělat, pokud ještě nejste v souladu s NIS2?

Neodkládejte to na později. Čím dříve začnete s přípravou, tím lépe.

Stanovte si realistický harmonogram a zajistěte dostatečné financování.

Proveďte analýzu rizik a posuďte stávající stav kybernetické bezpečnosti.

Využijte dostupné informační materiály a odborné konzultace.

Dva světy, jedna bitva: Zkušenosti matadorů a nejistota nově regulovaných subjektů

Zajímavý pohled nabízí výsledky v oblasti přístupu k regulaci. Obecně lze konstatovat, že společnosti, které jsou již regulovány jinými normami, přistupují k NIS2 systematicky a pragmaticky. Mají zkušenosti s implementací bezpečnostních opatření a vědí, jak je potřeba postupovat.

Nově regulované společnosti a odvětví odpovídají nekonzistentně a s nervozitou. Nemají zkušenosti s regulací kybernetické bezpečnosti a obávají se dopadu NIS2 na jejich fungování.

Dvě třetiny respondentů z oblasti digitálních služeb vnímá jako největší výzvu vysoké náklady na zajištění souladu s NIS2. To ukazuje, že firmy v tomto odvětví si uvědomují komplexnost regulace a nutnost investovat do technologií a procesů. Jiná odvětví (zejména výroba a zdravotnictví) uvádějí jako hlavní výzvu nedostatek personálních kapacit. To naznačuje, že firmám chybí odborníci na kybernetickou bezpečnost, kteří by jim pomohli s implementací NIS2.

Stejná situace je v oblasti očekávaných nákladů. Nově regulované společnosti očekávají navýšení nákladů na kybernetickou bezpečnost až o 40 %. To je značná suma, která může ohrozit jejich rozpočet.

Již regulované subjekty počítají s průměrným navýšením nákladů o 15 %. To ukazuje, že implementace NIS2 pro ně nebude tak nákladná, protože již dříve investovaly do kybernetické bezpečnosti.

Doporučení pro nově regulované společnosti:

Nepodléhejte panice a zpomalte. Udělejte si čas na analýzu aktuálního stavu a identifikujte nesoulady s požadavky NIS2.

Naplánujte investice do kybernetické bezpečnosti na příští rok. Není nutné hned nakupovat nové nástroje, ale je důležité nastavit efektivní procesy řízení bezpečnosti informací.

Začněte s GAP analýzou v první polovině roku 2024. To vám pomůže lépe se orientovat v požadavcích NIS2 a efektivněji plánovat implementaci.

Nezapomeňte, že důležitější, než nákup nástrojů je nastavení a implementace procesů. Kybernetická bezpečnost je o fungování celého systému, nejen o jednotlivých technologiích.

Využijte dostupné informační materiály a odborné konzultace. Existuje mnoho zdrojů, které vám pomohou s implementací NIS2.

Naše závěry

Nová regulace NIS2 představuje pro firmy výzvu, ale zároveň i příležitost k posílení kybernetické bezpečnosti. Společnosti, které se k ní postaví zodpovědně a systematicky, budou lépe chráněny před kybernetickými hrozbami, zároveň si zajistí soulad s legislativou a vylepší si svou obchodní pozici na trhu.

Dopad regulace na různé typy společností:

Nově regulované společnosti situaci vnímají složitěji a s jistou dávkou nervozity. Chtějí situaci vyřešit co nejdříve, ideálně do konce roku 2024.

Jiná situace je u regulovaných společností, kde k implementaci přistupují systematicky a s klidem. Mají předem stanovený harmonogram a kroky pro dosažení souladu. Většinou se spoléhají na interní zdroje a know-how.

Pozorujeme nedostatečné využívání publikovaných informací od NÚKIB a z veřejných zdrojů – pouze 7 % společností se obrací na NÚKIB pro informace o NIS2. To vede k nízké informovanosti o regulaci, NÚKIB je aktivní v poskytování informací a podpory firmám. Stejně tak můžete využít informace o NIS2 a praktické rady pro implementaci, které poskytujeme v rámci našich aktivit v EY.

Průzkum zároveň dotázaným umožnil vyjádřit svůj názor k přicházející regulaci NIS2 a mezi dotázanými bylo velké množství společností, které sdílejí problém s nedostatečným povědomím o přicházející regulaci, což se může velmi negativně podepsat na jejich budoucím fungování. I proto jsme se rozhodli Vám s tímto problémem pomoci. Naše společnost bude na toto téma připravovat několik workshopů. Sledujte naše webové stránky a neváhejte se zeptat. Informace o plánovaných workshopech bude brzy zveřejněna.

NIS2 bez kompromisů: S EY dosáhnete souladu a posílíte kybernetickou odolnost

Analýza a implementace požadavků směrnice NIS2 a souvisejícího Zákona o kybernetické bezpečnosti, vnímáme jako komplexní aktivitu. Pro účely efektivní dodávky služeb v oblasti analýzy souladu a implementace požadavků NIS2 vznikla pracovní skupina evropských týmů EY, kde se sdílejí zkušenosti z mnoha mezinárodních projektů.

V rámci našich služeb tak využíváme různé pohledy na řízení a implementaci kybernetické bezpečnosti z obdobných projektů v celé Evropě. Náš tým EY Česká republika se skládá ze zkušených profesionálů s odborností ve všech relevantních oblastech – IT bezpečnost, bezpečnostní architektura, analýza souladu a implementace systému řízení bezpečnosti informací, právní expertíza v oblasti kybernetické bezpečnosti a procesní řízení.

Kybernetickou bezpečnost vnímáme jako nedílnou součást firemní politiky.

Za účelem realizace projektů souvisejících s analýzou souladu vůči požadavkům NIS2 (potažmo prováděcí legislativy) vznikly interní nástroje EY, jenž umožňují systematické, efektivní ale zejména komplexní provádění zhodnocení souladu.

Interní NIS2 assessment tool

Aplikace využívající technologie Microsoft.

Set dotazů a očekávaných odpovědí, vycházející z VoKB, ISO/IEC 27001.

Sjednocené hodnocení s NIS2 nástrojem s očekávanými odpověďmi.

Hodnocení souladu založeno formou výběru ze stavů (odpověď je plně v souladu, převážně v souladu, částečně v souladu, nebo v nesouladu).

EY eXtreme Hacking - Testování kybernetické odolnosti

Doplnění GAP analýzy, ověření schopnosti bezpečnostních týmů, a souladu nastavení bezpečnostních nástrojů.

Ověření funkčnosti a efektivity procesů v praxi jako doplňěk GAP analýzy.

Simulace kroků skutečných útočníků.

Potřebné kroky pro zajištění souladu

01 GAP analýza

02

- Aktualizace stávající bezpečnostní dokumentace, struktury a odpovědností
- Aktualizace stávajících bezpečnostních postupů
- Testování kybernetické odolnosti a schopnosti reakce na kybernetické incidenty
- Identifikace rizik spojených s třetími stranami
- Zajištění kontinuity regulovaných služeb

Celkové ověření shody s NIS2 lze rozdělit do 3 projektových fází

Fáze 1
Identifikace regulovaných služeb a dopadu NIS2

Cílem fáze 1 je zjistit, zda a jak se na společnost vztahuje směrnice NIS2, identifikovat všechny regulované služby, které společnost má, a posoudit rozsah dopadu NIS2 na danou společnost. Regulované služby dále kategorizujeme dle typu a úrovně dopadu.

Fáze 2
Dokumentace, procesy a jejich design

Fáze 2 má za cíl přezkoumat soulad interní bezpečnostní dokumentace a design navržených procesů. To zahrnuje zhodnocení kvality a nezbytných parametrů interních bezpečnostních procesů vůči požadavkům ZoKB a VoKB a dalších bezpečnostních norem.

Fáze 3
Efektivita bezpečnosti v praxi

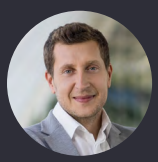
Fáze 3 ověřuje efektivitu fungování klíčových bezpečnostních procesů, dále pak fungování procesů na vzorku vybraných aktiv, které podporují regulované služby a také praktické testování detekčních schopností.

Nebojte se, s námi to zvládnete

Kybernetická bezpečnost a NIS2: Nečekejte do poslední chvíle! Už letos by se firmy měly aktivně zabývat směrnicí NIS2 a provést GAP analýzu. Ta jim ukáže, jak si stojí v oblasti kybernetické bezpečnosti ve srovnání s požadavky směrnice. Zároveň identifikuje oblasti, kde je nutné dosáhnout souladu, ať už plného, nebo částečného.

Čím dříve se firmy začnou problematikou NIS2 zabývat, tím více času budou mít na implementaci potřebných opatření a dosažení souladu.

Petr Plecháček
Consulting | Technology Consulting
Partner, EY
petr.plechacek@cz.ey.com



Jan Pich
Consulting | Technology Consulting
Cyber Security Senior Manager, EY
jan.pich@cz.ey.com