Digital Security
Progress. Protected.

EVERSHEDS SUTHERLAND

NIS2

Nejnovější legislativa EU pro oblast kybernetické bezpečnosti

AKTUALIZOVÁNO

Spoluautoři:
Saranda Walgaard
Andre Lamerias

OBSAH

Co je směrnice NIS2?

Směrnice NIS2 posiluje kybernetickou bezpečnost v celé EU. Tato aktualizovaná verze první směrnice o síťových a informačních systémech (NIS) vstoupila v platnost 16. ledna 2023 a vyžaduje, aby subjekty působící v kritických odvětvích, jako je energetika, doprava, zdravotnictví, digitální služby a řízené bezpečnostní služby (MSSP), zavedly efektivnější řízení rizik. NIS2 rovněž zavádí nová pravidla pro hlášení incidentů a systém sankcí a donucovacích prostředků.

Směrnice NIS a NIS2: Vývoj regulací kybernetické bezpečnosti v EU

Původní směrnice NIS přijatá v roce 2016 představovala první legislativu týkající se kybernetické bezpečnosti platnou pro všechny členské státy Evropské unie. Soustředila se zejména na dvě skupiny organizací: jednak na provozovatele základních služeb (zdravotnictví, doprava, energetika atd.), a jednak na poskytovatele digitálních služeb, kam spadají online vyhledávače, internetová tržiště nebo cloudové služby. Směrnice NIS od těchto organizací vyžadovala plnění odpovídajících bezpečnostních opatření a nahlášení každého většího incidentu v oblasti kybernetické bezpečnosti, který zaznamenají. Zároveň ale dávala prostor jednotlivým státům zohlednit místní podmínky.

Směrnice NIS2 vytváří nový rámec s cílem posílit úroveň kybernetické bezpečnosti v celé Evropské unii. Tato aktualizovaná verze původní směrnice o sítích a informačních systémech vstoupila v platnost 16. ledna 2023 a bude zahrnovat nejen členské státy EU, ale také organizace mimo EU, které hrají na jejím trhu zásadní roli. Od podniků, působících ve vysoce kritických odvětvích, bude požadováno, aby přijaly jak technická, tak provozní opatření s cílem splnit nároky směrnice NIS2, **včetně reakce na incidenty, zabezpečení dodavatelského řetězce, šifrování a ohlašování zranitelností, přiměřené analýzy rizik, testování a auditování strategií kybernetické bezpečnosti a plánování krizového řízení tak, aby byl zajištěný kontinuita činností podniku.** V případě narušení bezpečnosti se bude od těchto subjektů požadovat, aby do 24 hodin od incidentu zveřejnily prvotní oznámení a do 72 hodin pak podrobnější informace. Směrnice NIS2 zároveň zavádí systém sankcí za nedodržení těchto požadavků, včetně pozastavení certifikace a vyvození osobní odpovědnosti pracovníků na manažerských pozicích, v souladu s národní legislativou.

Které sektory zahrnovala směrnice NIS?

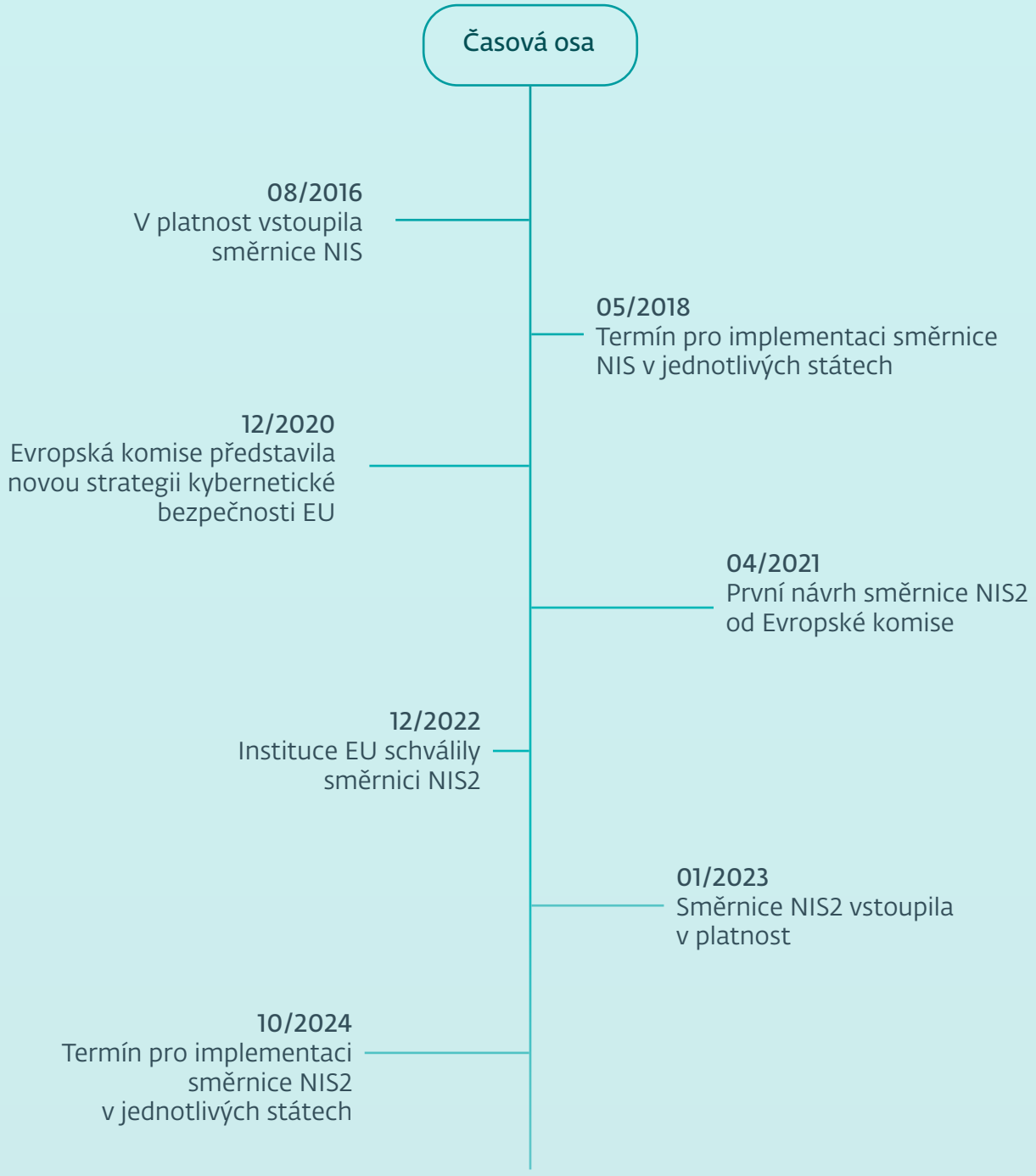
- Zdravotnictví
- Digitální infrastruktura
- Doprava
- Dodávka vody
- Poskytovatelé digitálních služeb
- Infrastruktura bankovnictví a finančních trhů
- Energetika

Které sektory jsou přidané ve směrnici NIS2?

- Poskytovatelé poskytovatelé digitální infrastruktury
- Odpadní voda a odpadní hospodářství
- Výroba určitých kritických produktů (např. farmaceutika, zdravotnická zařízení a chemické látky)
- Potravinářství
- Digitální služby (např. platformy sociálních sítí a služby datových center)
- Vesmír
  *ČR se tento sektor netýká
- Poštovní a kurýrní služby
- Veřejná správa

Směrnice také ustanovuje **Evropskou síť styčných organizací pro řešení kybernetických krizí** EU-CyCLONe (European Cyber Crises Liaison Organization Network), která má umožnit spolupráci mezi národními úřady a orgány zodpovědnými za kybernetickou bezpečnost. Od každého členského státu se navíc bude požadovat, aby jasně určil jedno kontaktní místo, kam se budou kybernetické incidenty hlásit.

Směrnice NIS2 nabude účinnosti, jakmile ji členské státy EU přenesou do své národní legislativy, což mají provést do září 2024. Organizacím se nicméně doporučuje připravit se raději dříve než později: nejen proto, aby proces implementace zvládly včas, ale také aby měly prostor otestovat různé osvědčené postupy při zvládání incidentů a zásady řízení a vyrovnat se s mýty, které panují v otázkách hlášení incidentů.



Kdo má povinnost se směrnicí řídit?

V porovnání s předchozí verzí nová směrnice NIS ruší rozdíl mezi poskytovateli základních služeb a poskytovateli služeb digitálních. Subjekty klasifikuje podle důležitosti a dělí do dvou kategorií podléhajících odlišným dohledovým režimům: na základní (essential) a důležité (important).

Znamená to, **že všechny odvětví a služby spadající pod směrnici NIS2 mají pro evropskou společnost vysokou důležitost. Má se za to, že přerušení jejich provozu a situace, kdy by nadále nemohly plnit své funkce,** by společnosti způsobily značné škody. Zmíněné dvě kategorie byly vytvořené s cílem odlišit různou míru dopadu případného incidentu na společnost v různých sektorech.

Kterých odvětví se směrnice týká?

NIS2 požaduje zabezpečit všechny služby důležité pro fungování společnosti.
Tyto služby uvádí směrnice NIS2 ve svých přílohách I a II.

Základní subjekty

Subjekty uvedené **v příloze I**.

Mezní hodnoty pro velké organizace

počet zaměstnanců > 250
obrat > 50 mil. eur
aktiva > 43 mil. eur

Sektory s vysokou kritičností

- Energetika
- Doprava
- Bankovnictví
- Poskytovatelé řízených ICT služeb
- Pitná voda
- Odpadní voda
- Zdravotnictví
- Digitální infrastruktura
- Veřejná správa
- Infrastruktura finančních trhů
- Vesmír

Důležité subjekty

Subjekty uvedené **v příloze II**.

Mezní hodnoty pro středně velké organizace

50–250 zaměstnanců
obrat 10–50 milionů eur
aktiva < 43 mil. eur

Další kritické sektory

- Poštovní a kurýrní služby
- Odpadní hospodářství
- Chemický průmysl
- Potravinářství
- Výroba elektronických a optických přístrojů aj.
- Poskytovatelé digitálních služeb
- Výzkum

Oba typy subjektů mají stejné povinnosti a závazky. Členové managementu základních a důležitých subjektů tak mají například povinnost absolvovat školení a subjekty musí přijmout náležitá a přiměřená technická, provozní a organizační opatření k řízení rizik ohrožujících bezpečnost jejich sítí a informačních systémů. Tato opatření pak budou využívat při provozu či zajišťování služeb tak, aby předcházely bezpečnostním incidentům nebo minimalizovaly jejich dopad na příjemce svých služeb.

Od základních organizací se také bude požadovat, aby měly proaktivně připravený rámec k vyhodnocení nevhodného řízení i v případě, že k incidentu nedojde. Od důležitých subjektů se dodržování pravidel očekává reaktivně, jinými slovy, soulad se zákony a dalšími předpisy se u těchto organizací bude prověřovat po případném incidentu. Pokud šetření dojde k závěru, že organizace nepodnikla dostatečné kroky a nesplnila požadavky, budou se u obou typů subjektů uplatňovat sankce.

Je důležité vědět, že do 17. dubna 2025 (a poté každé dva roky) informují kompetentní orgány Evropskou komisi a Skupinu pro spolupráci (Cooperation Group) o počtu základních a důležitých subjektů v jednotlivých sektorech.

Povinnost řádné péče a oznamovací povinnost

Všechny organizace spadající pod směrnici NIS2, tj. základní i důležité, budou muset začít plnit svou povinnost řádné péče. Směrnice obsahuje seznam typů opatření, která musí poskytovatelé služeb dodržet jako povinné minimum. Patří k nim vyhodnocování rizik s cílem zjistit, jestli organizace věnuje dostatečnou pozornost zabezpečení informačních systémů, krizovému řízení a zajištění kontinuity činností v případě závažného kybernetického incidentu a jestli dokáže zajistit zabezpečení svého dodavatelského řetězce. Povinnost řádné péče dále zahrnuje zabezpečení sítě a informačních systémů s využitím kryptografických a šifrovacích metod a zavedení zásad a postupů, k hodnocení efektivity opatření v oblasti řízení rizik. Také oznamovací povinnost se týká všech organizací spadajících pod směrnici NIS2. Tento závazek ohlašovat incidenty žádá od dotčených organizací, aby incident nahlásily příslušným orgánům do 24 hodin od jeho zjištění, do 72 hodin od podání prvního hlášení dodaly podrobnější aktuální informace o incidentu a zavedených opatřeních, a do jednoho měsíce od podání prvního oznámení předložily závěrečnou zprávu.

Povinnost řádné péče

Podle původní směrnice NIS se povinnost řádné péče týká jak poskytovatelů základních služeb, tak poskytovatelů služeb digitálních. Oba typy subjektů musí přijmout náležitá a přiměřená technická, provozní a organizační opatření k řízení rizik ohrožujících bezpečnost jejich sítí a informačních systémů.

Nová směrnice NIS2 přichází s jiným typem rozlišení: na základní a důležité subjekty. To odráží míru, do jaké je daný subjekt kritický v rámci konkrétního odvětví nebo typu služeb, a také velikost subjektu. Plnění povinnosti řádné péče se bude opět požadovat od obou typů subjektů. Sestavení seznamu základních a důležitých subjektů je na členských státech. Povinnost registrace, resp. hlášení nezbytných údajů a incidentů byla obsažena již v původním zákoně o kybernetické bezpečnosti, nový návrh zákona toto jen detailněji upravuje. Subjekty začnou podléhat opatřením cíleným na řízení rizik v oblasti kybernetické bezpečnosti ve chvíli, kdy se zaregistrují v jedné ze dvou uvedených kategorií. Opatření by měla odpovídat míře vystavení základního či důležitého subjektu rizikům a společenskému a ekonomickému dopadu, který by měl případný incident. V potaz je třeba vzít také kritičnost daného subjektu, jeho velikost a pravděpodobnost vzniku incidentů.

V této souvislosti se zabezpečením rozumí schopnost sítě a informačních systémů odolat činnostem, které narušují jejich dostupnost, autenticitu, integritu a důvěrnost. Prováděcí nařízení Komise (nařízení (EU) 2018/151) dále specifikuje prvky zabezpečení, které je třeba dodržovat: zabezpečení systémů a fyzická bezpečnost, zvládání incidentů, řízení kontinuity provozu, monitorování, audity a testování a mezinárodní normy

Směrnice NIS2 shrnuje minimální sadu opatření, včetně provádění analýzy rizik a zavedení zásad zabezpečení informačních systémů, zvládání incidentů, kontinuity provozu a krizového řízení, zabezpečení dodavatelského řetězce a zabezpečení při nákupu, vývoji, údržbě sítí a informačních systémů. Součástí jsou také zásady a postupy hodnocení efektivity opatření při řízení rizik a využití kryptografie a šifrování.

Základní i důležité subjekty **by také měly přijmout širokou škálu základních postupů kybernetické hygieny, jako je princip nulové důvěry, aktualizace softwaru, konfigurace zařízení, segmentace sítě, řízení identit a přístupů nebo vzdělávání uživatelů, pořádání školení pro zaměstnance a zvyšování povědomí o kybernetických hrozbách, phishingu nebo technikách sociálního inženýrství.** Subjekty by také měly znovu zhodnotit nasazená řešení kybernetické bezpečnosti a v případě potřeby integrovat technologie posilující bezpečnost, jako jsou například systémy umělé inteligence či strojového učení, které rozšíří dostupné možnosti a zlepší zabezpečení sítí a informačních systémů.

S ohledem na prokázání souladu s těmito opatřeními **můžou členské státy navíc od základních a důležitých subjektů také vyžadovat používání konkrétních produktů ICT, služeb či procesů, které budou certifikované podle evropských systémů certifikace kybernetické bezpečnosti** přijatých na základě aktu o kybernetické bezpečnosti (nařízení (EU) 2019/881)

Evropská komise má navíc pravomoc přijímat prováděcí akty a akty v přenesené pravomoci, které dále specifikují opatření pro řízení rizik. Proto mohou být povinnosti zpřesňovány s ohledem na nové kybernetické hrozby, technologický vývoj nebo specifika jednotlivých sektorů.

Oznamovací povinnost

S příchodem směrnice NIS2 se vedle povinnosti řádné péče dále rozvine i oznamovací povinnost, která existovala už v rámci původní směrnice NIS.

První směrnice NIS zavedla povinnost oznamovat incidenty s významným dopadem na kontinuitu služeb. Podle směrnice se incidentem rozumí „jakákoli událost, která má reálný negativní dopad na bezpečnost sítí a informačních systémů". Zabezpečením se pak rozumí „schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují jejich dostupnost, autenticitu, integritu nebo důvěrnost". **Pro účely hodnocení, jestli má incident významný dopad, popisuje dokument několik parametrů, které je třeba zvážit, včetně počtu zasažených uživatelů, doby trvání incidentu a velikosti zasažené geografické oblasti.** Pokud se z pohledu dodavatele jeví, že incident má významný dopad na kontinuitu poskytovaných služeb, **, je nutné ho neprodleně nahlásit místnímu týmu CSIRT (Computer Security Incident Response Team) nebo kompetentnímu orgánu určenému členským státem.** Hlášení musí obsahovat dostatečné informace, které kompetentnímu orgánu nebo týmu CSIRT umožní určit přeshraniční dopad incidentu.

Směrnice NIS2 nařizuje při ohlašování incidentů „dvoustupňový přístup".
Cílem prvního oznámení je omezit potenciální šíření incidentů a umožnit subjektům vyhledat podporu. Druhé oznámení by pak mělo být podrobné a mělo by zajistit možnost poučit se z předchozích incidentů. Je ovšem důležité poznamenat, že někdy může být nutné další upřesnění, aby mohly být incident a jeho dopady důsledně zhodnoceny. Dalším cílem je postupně posilovat odolnost jednotlivých společností a celých odvětví vůči kybernetickým hrozbám.

Fáze oznamování incidentů podle směrnice NIS2

Do 24 hodin od zjištění incidentu (a bez zbytečného prodlení) by mělo být kompetentnímu orgánu nebo příslušnému týmu CSIRT pro daný stát předáno první oznámení. Pokud je to možné, mělo by uvádět, jestli incident způsobilo nezákonné nebo škodlivé jednání. Toto ustanovení zajišťuje předání nezbytných informací.

Do 72 hodin od prvního oznámení má zasažený subjekt povinnost předložit aktuální informace a prvotní hodnocení, které bude obsahovat podrobnosti o útoku a opatření zavedená v reakci na něj. Pokud si to subjekt vyžádá, může získat rady k možným opatřením na zmírnění situace a v případě potřeby také další technickou podporu. V případě trestného činu získá zasažený subjekt také poradenství, jak incident oznámit orgánům činným v trestním řízení.

Do jednoho měsíce od podání prvního oznámení je pak nutné předložit závěrečnou zprávu, která bude obsahovat:

- podrobný popis incidentu, jeho závažnosti a důsledků,
- typ hrozby nebo jiné příčiny, která k incidentu pravděpodobně vedla,
- okamžitá a průběžně uplatňovaná opatření na zmírnění

V rámci směrnice NIS2 bylo přijato ustanovení o oznamování incidentů s významnými dopady. To upřesňuje, **že subjekty budou mít také povinnost nahlásit všechny významné kybernetické hrozby, které by mohly vést k významnému incidentu**. Pokud jde o pojem „kybernetická bezpečnost", řídí se definicí formulovanou v nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti"). Toto nařízení definuje kybernetickou bezpečnost jako „činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a osob dotčených kybernetickými hrozbami". Incident se pak pokládá za závažný, pokud jeho výsledkem jsou nebo můžou být závažná narušení provozu nebo finanční ztráty pro dotčený subjekt nebo pokud se incident dotkl nebo mohl dotknout fyzických či právnických osob způsobením závažných materiálních nebo nemateriálních škod.

Subjekty, kterých se směrnice NIS2 netýká, můžou dobrovolně oznamovat závažné incidenty, kybernetické hrozby nebo situace, kdy se jim těsně vyhnuly. Kompetentní orgán nebo tým CSIRT se budou řídit postupem popsaným v části „dvoustupňové oznámení". Dobrovolně předložená oznámení nemají podléhat žádným dalším povinnostem. Pokud tedy subjekt učiní dobrovolné oznámení, neměly by mu vzniknout náročnější závazky než v případě, že by oznámení nepodal.

Jak to bude fungovat?

Jakmile členské státy začlení směrnici NIS2 do své národní legislativy, je na nich, aby zajistily účinný dohled nad plněním jejích požadavků.

U základních subjektů se jedná o dohled proaktivní. Naopak důležité subjekty podléhají dohledu reaktivnímu, **ke kterému můžou dát podnět na základě důkazů, indicií či informací či informace, že subjekt směrnici údajně nedodržuje**. Ve druhém případě je skutečně nutné podniknout nějaké kroky, jen pokud se zdá, že důležitý subjekt neplní závazky vyplývající ze směrnice.

Definice základních a důležitých subjektů najdete v tabulce na straně 5

Opatření přijatá kompetentními orgány musí být účinná a přiměřená a musí odrazovat od podobného jednání. U obou typů subjektů **budou mít kompetentní orgány pravomoc podrobit je kontrole na pracovišti a zpětné kontrole mimo pracoviště, kterou povedou vyškolení odborníci, cíleným bezpečnostním auditům a zběžným kontrolám zabezpečení. Můžou požadovat vyhovění požadavkům na přístup k datům, dokumentům a informacím a požadavkům na předložení důkazů o zavedení zásad kybernetické bezpečnosti, jako jsou výsledky bezpečnostních auditů provedených oprávněným auditorem a související podkladová dokumentace**. Seznam kontrol v případě základních subjektů dále rozšiřují náhodné kontroly a ad hoc audity. S výjimkou řádně odůvodněných případů ponesou náklady bezpečnostních auditů auditované subjekty.

Pokud se zjistí porušení pravidel, můžou kompetentní orgány uplatnit další donucovací prostředky, například vydat varování, stanovit pokyny, nařídit subjektům, aby upustily od činností porušujících směrnici, nařídit subjektům informovat fyzické či právnické osoby, které mohly být nevhodným jednáním dotčeny, nebo informace o porušení zveřejnit. V případě, že by tato opatření nevedla k nápravě situace, můžou kompetentní orgány dočasně pozastavit činnosti subjektu a zbavit funkce jeho manažera, který vykonává povinnosti na právní úrovni výkonného ředitele či zástupce subjektu.

Směrnice NIS2 stanovuje konzistentní rámec sankcí pro celou Unii. Určuje totiž minimální seznam administrativních sankcí za porušení povinností spojených s řízením rizik v oblasti kybernetické bezpečnosti a jejich oznamováním. Tyto sankce zahrnují závazné pokyny, implementaci doporučení z bezpečnostního auditu, sladění bezpečnostních opatření s požadavky směrnice NIS2 a správní pokuty.

Členské státy musí relevantním orgánům poskytnout pravomoc udělit značné pokuty. U základních subjektů se jedná o maximálně 10 000 000 € nebo nejméně 2 % celosvětového ročního obratu za předchozí finanční rok, podle toho, která částka je vyšší. Pokud jde o důležité subjekty, maximální pokuta je stanovená na 7 000 000 € nebo nejméně 1,4 % celosvětového ročního obratu za předchozí finanční rok, podle toho, která částka je vyšší.

Odpovědnost za nedodržení ustanovení směrnice NIS2 můžou nést také řídicí orgány základních a důležitých subjektů. Pokud vaše organizace podléhá směrnici a nedokáže nastavit nebo udržovat kybernetickou bezpečnost v dobrém stavu, budou jí uděleny pokuty a sankce za nedodržení opatření při řízení rizik nebo oznamovacích povinností

Pro posílení dohledu, který napomáhá účinnému dodržování pravidel, shrnuje směrnice NIS2 minimální seznam dohledových prostředků, které můžou kompetentní orgány použít při výkonu dohledu nad základními i důležitými subjekty. Ty zahrnují pravidelné a cílené audity, kontroly na pracovišti i mimo něj, žádosti o informace a přístup k dokumentům a důkazům.

Při uplatňování svých donucovacích pravomocí musí kompetentní orgány přihlížet ke konkrétním okolnostem každého případu, jako je povaha, závažnost a délka porušení, způsobené škody či vzniklé ztráty a to, jestli k porušení došlo záměrně nebo z nedbalosti.

Aby byla zajištěná odpovědnost za opatření v oblasti kybernetické bezpečnosti na úrovni organizace, **zavádí směrnice NIS2 ustanovení o odpovědnosti fyzických osob zastávajících pozice** ve vyšším managementu subjektů, které pod směrnici spadají.

Co směrnice NIS2 znamená pro malé a střední podniky?

Směrnice NIS2 zavádí uplatňování pravidla velikostních limitů tak, jak jsou definované v tabulce na straně 5. I když vyjímá z povinnosti dodržovat nová pravidla většinu malých a středních podniků, existují určité výjimky. **Například pro malé a střední podniky v sektorech sítí pro elektronickou komunikaci nebo veřejně dostupné služby elektronické komunikace, poskytovatele služeb zajišťujících důvěru nebo poskytovalele registrů domén nejvyššího řádu (TLD).**

Malé a střední podniky se stále častěji stávají cílem útoků na dodavatelský řetězec, protože v oblasti zabezpečení disponují omezenými zdroji. Podobné útoky na dodavatelský řetězec můžou mít dominový efekt a přenést se na subjekty, kterým tyto podniky poskytují služby. **Členské státy proto musí prostřednictvím svých národních strategií kybernetické bezpečnosti pomáhat malým a středním podnikům vyrovnávat se s výzvami, kterým ve svých dodavatelských řetězcích čelí**. Členské státy by pro malé a střední podniky měly mít národní nebo oblastní kontaktní místo, které jim buď bude poskytovat poradenství a pomoc s problémy souvisejícími s kybernetickou bezpečností, nebo je nasměruje na vhodné instituce, které jim takovou pomoc poskytnou.

V březnu 2021 Evropská aliance DIGITAL SME, největší síť malých a středních podniků z oboru ICT v EU, publikovala prohlášení k návrhu směrnice NIS2, ve které novou směrnici uvítala, ale zároveň upozornila na její nepřímé dopady na malé a střední podniky.

Podle Jamese Philpota, projektového manažera sdružení DIGITAL SME, **je prvním krokem, který by malé a střední firmy měly podniknout, aby pochopily specifické potřeby při zdokonalování svých postupů v oblasti kybernetické bezpečnosti, prostudování průvodců a doporučení** národních center kybernetické bezpečnosti a agentury ENISA. Avšak získat správné informace může být více či méně náročné, protože různé členské státy poskytují různé zdroje. Směrnice NIS2 nicméně státy zavazuje k poskytování podpory a zdrojů, zejména pokud jde o získání podrobného přehledu o rozsahu této legislativy a o tom, jestli jí podniky podléhají, což napomůže včasnému plánování.

„Největší narušení provozu zřejmě pocítí poslední článek dodavatelského řetězce (tj. distributoři). Pro některé společnosti tak může být náročné nejen zajistit potřebné technické prostředky, ale také porozumět požadavkům na oznamování incidentů a na to, jak směrnice NIS2 funguje v kontextu další legislativy", vysvětlil Philpot.

Sebedůvěra malých a středních podniků v oblasti kybernetické odolnosti

Jen 48 % malých a středních podniků tvrdí, že v oblasti kybernetické odolnosti pociťují středně velkou nebo velkou úroveň sebedůvěry

7 % | vůbec žádná sebedůvěra

10 % | velká úroveň sebedůvěry

38 % | středně velká úroveň sebedůvěry

45 % | nízká úroveň sebedůvěry

74 % malých a středních podniků je přesvědčeno, že jsou kvůli své velikosti zranitelnější vůči kybernetickým útokům než velké podniky

Zdroj: Zpráva SMB's Digital Security Sentiment společnosti ESET (2022)

Obecně vzato bychom měli vítat veškeré snahy zvýšit úroveň kybernetické bezpečnosti evropských podniků. Sdružení DIGITAL SME i společnost ESET jsou přesvědčené, že tento nový legislativní rámec by tomu mohl pomoci. Jediné riziko, jak upozorňuje Philpot, je úroveň implementace a podpory. Právě na jejich zvládnutí bude záviset to, jestli nová legislativa malým a středním podnikům pomůže, nebo je naopak nadměrně zatíží.

V Evropě jsou dostupná technická řešení zajišťující požadovanou úroveň kybernetické bezpečnosti, společnosti by ale neměly hledat největšího poskytovatele ani nejlevnější nabídku – obojí obvykle přichází od firem mimo Evropu. Z tohoto důvodu je velmi důležité propojit podporu a zdroje při využití této legislativy a posílit evropské inovace.

Malé a střední podniky se můžou obrátit také na místní týmy CSIRTs které jim můžou pomoct v oblastech, v nichž nezískaly dostatečnou podporu od jiných národních orgánů, případně využít zdroje, jako je DIGITAL SME/SBS guide, the DIGITAL SME Guide on Information Security Controls nebo certifikace pro kybernetickou bezpečnost.

Hlavní obavy malých a středních podniků z obchodních dopadů kybernetického útoku

Source: ESET SMB's Digital Security Sentiment Report (2022)

Jak dále poznamenal James Philpot v rozhovorech se zástupci společnosti ESET, malé a střední podniky dobře znají dopady kybernetických incidentů a vědí, že je můžou potkat úniky dat, citelné finanční ztráty nebo ztráta důvěry zákazníků. Jako naprosté minimum tak můžou vzít směrnici NIS2 jako příležitost k rozvíjení povědomí o této oblasti a posílení své kybernetické odolnosti.

Rady a tipy společnosti ESET pro digitální zabezpečení malých a středních podniků můžete sledovat na stránkách Digital Security Guide

Jaké povinnosti přinese nový Zákon o kybernetické bezpečnosti?

Kdy budou společnosti muset začít plnit požadavky NIS2?

Členské státy EU musí požadavky NIS2 přenést do svých vnitrostátních právních předpisů do 17.října 2024. V ČR budou požadavky NIS2 zapracované v nové verzi Zákona o kybernetické bezpečnosti (ZKB).

Kde se mají společnosti k povinnostem zaregistrovat?

Ode dne účinnosti nového ZKB začne organizacím, které splňují kritéria poskytovatele regulované služby, běžet lhůta, kdy se musí registrovat u Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Registraci musí společnosti provést nejpozději do 30 dnů ode dne, kdy zjistí, že došlo k naplnění kritérií pro identifikaci regulované služby, nejpozději však do 90 dnů ode dne, kdy k naplnění kritérií pro identifikaci regulované služby došlo.

NÚKIB poté pošle registrovaným společnostem vyrozumění o zápisu regulované služby. Následně začne běžet lhůta 1 roku, během které musí společnost zavést odpovídající bezpečnostní opatření.

Jak ZKB rozděluje povinné subjekty a jak zjistím, jestli mezi ně patřím?

Zákon o kybernetické bezpečnosti rozděluje poskytovatele regulované služby, kteří naplní daná kritéria, do dvou kategorií – režimu **nižších** nebo **vyšších povinností**.

Kritéria pro identifikaci regulovaných služeb a stanovení režimů poskytovatele regulované služby budou uvedena v podzákonném prováděcím předpisu – Vyhlášce o regulovaných službách.

PŘEJÍT NA WEB

Chcete zjistit, jestli patříte mezi poskytovatele regulované služby a do jakého režimu spadáte?

Zkuste to na našem webu, kde po vyplnění krátkého dotazníku dostanete předběžnou odpověď.

Jaká bezpečnostní opatření musí poskytovatele regulované služby zavést?

Režim vyšších povinností

1. organizační opatření

a. systém řízení bezpečnosti informací,
b. povinnosti vrcholného vedení,
c. bezpečnostní role,
d. řízení bezpečnostní politiky a bezpečnostní dokumentace,
e. řízení aktiv,
f. řízení rizik,
g. řízení dodavatelů,
h. bezpečnost lidských zdrojů,
i. řízení změn,
j. akvizice, vývoj a údržba,
k. řízení přístupu,
l. zvládání kybernetických bezpečnostních událostí a incidentů,
m. řízení kontinuity činností a
n. audit kybernetické bezpečnosti,

2. technická opatření

a. systém řízení bezpečnosti informací,
b. povinnosti vrcholného vedení,
c. bezpečnostní role,
d. řízení bezpečnostní politiky a bezpečnostní dokumentace,
e. řízení aktiv,
f. řízení rizik,
g. řízení dodavatelů,
h. bezpečnost lidských zdrojů,
i. řízení změn,
j. akvizice, vývoj a údržba,
k. řízení přístupu,
l. zvládání kybernetických bezpečnostních událostí a incidentů,
m. řízení kontinuity činností a
n. audit kybernetické bezpečnosti,

Režim nižších povinností

a. zajišťování kybernetické bezpečnosti,
b. povinnosti vrcholného vedení,
c. řízení aktiv,
d. řízení rizik,
e. bezpečnost lidských zdrojů,
f. řízení kontinuity činností,
g. řízení přístupu,
h. řízení identit a jejich oprávnění,
i. detekce a zaznamenávání kybernetických bezpečnostních událostí,
j. řešení kybernetických bezpečnostních incidentů,
k. bezpečnost komunikačních sítí,
l. aplikační bezpečnost a
m. kryptografické algoritmy.

Vybrané příklady bezpečnostních opatření

Bezpečnost lidských zdrojů

Společnost musí s ohledem na stav a potřeby systému řízení bezpečnosti informací stanovit **plán rozvoje bezpečnostního povědomí**. Plán musí zahrnovat vrcholové vedení, uživatele, administrátory, osoby zastávající bezpečnostní role a dodavatele a musí obsahovat poučení o jejich povinnostech a bezpečnostní politice, ale např. také pravidla tvorby bezpečných hesel.

Povinnosti vrcholného vedení

Mezi povinnosti vrcholného vedení společnosti se řadí např. **prokazatelná účast** na školení (vstupních a pravidelných), kde dojde k poučení vrcholného vedení o jeho povinnostech, o bezpečnostní politice zejména v oblasti systému řízení bezpečnosti informací a řízení rizik.

Dále musí vrcholné vedení zajistit stanovení pravidel pro určení administrátorů a osob, které budou zastávat **bezpečnostní role** a tyto osoby dále podporovat při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti. Musí určit osoby, které budou zastávat následující bezpečnostní role, které jsou také v Zákoně definovány:

a. manažer kybernetické bezpečnosti,
b. architekt kybernetické bezpečnosti,
c. garant aktiva a
d. auditor kybernetické bezpečnosti.

Řízení aktiv

Společnost musí stanovit metodiku pro identifikaci a hodnocení aktiv, a určit a evidovat **garanty** aktiv. Primární aktiva hodnotí podle CIA triády (důvěrnosti, integrity a dostupnosti) a zařazuje je do jednotlivých úrovní. Pro jednotlivé úrovně aktiv zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, integrity a dostupnosti.

Řízení rizik

Společnost musí stanovit metodiku pro identifikaci a hodnocení rizik. Při identifikaci rizik s ohledem na aktiva identifikuje relevantní hrozby a zranitelnosti. Hodnocení rizik bude společnost provádět alespoň jednou ročně. Na základě hodnocení rizik a bezpečnostních potřeb zpracuje zprávu o hodnocení rizik, prohlášení o aplikovatelnosti a plán zvládání rizik.

Správa a ověřování identit

Mezi povinnosti společnosti při správě a ověření identity administrátorů, uživatelů a technických aktiv regulované služby spadá používání nástroje, který mimo jiné zajistí ověření identity před zahájením aktivit, řízení počtu neúspěšných pokusů o přihlášení, opětovné ověření identity po stanovené době nečinnosti a odolnost uložených a přenášených autentizačních údajů. Autentizační mechanismus, který společnost používá, musí být založen **na vícefázovém ověřování s nejméně dvěma různými typy faktorů**.

Detekce a vyhodnocování kybernetických bezpečnostních událostí

Společnost musí používat **nástroj pro detekci kybernetických bezpečnostních událostí**, který disponuje ověřováním a kontrolou přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi, na síťovém perimetru a zajišťuje blokování nežádoucí komunikace. Centrálně spravovaný nástroj s ohledem na vazby mezi aktivy mimo jiné musí zajistit **nepřetržitou a automatickou ochranu před škodlivým kódem** (na jednotlivých relevantních technických aktivech, zejména na serverech a koncových stanicích), řízení a sledování používání vyměnitelných zařízení a datových nosičů, řízení automatického spuštění obsahu (zejména u vyměnitelných zařízení a datových nosičů), řízení a sledování komunikace aplikací, jejich služeb a detekci na základě chování technického aktiva, administrátorů a uživatelů.

Dále musí nepřetržitě poskytovat informace o detekovaných kybernetických událostech, **včasné varování** určených bezpečnostních rolí a vyhodnocování událostí s cílem **identifikace kybernetických bezpečnostních incidentů**.

Používaný nástroj musí být **pravidelně aktualizován**, včetně jeho pravidel pro detekci a vyhodnocování událostí a pro nepřetržité poskytování informací o detekovaných událostech.

Aplikační bezpečnost

Povinnosti v oblasti aplikační bezpečnosti přestavují pro společnost bezodkladné aplikování bezpečnostních **aktualizací pro technická aktiva** a také **skenování zranitelností** těchto aktiv. S ohledem na hodnocení technických aktiv a jejich rizik musí společnost také provádět jejich **penetrační testování** a na základě jeho výsledků zavést bezpečnostní opatření.

Jaké další povinnosti Zákon přináší?

Mechanismus prověřování dodavatelského řetězce

Pokud vaše společnost patří mezi poskytovatele regulované služby **v režimu vyšších povinností** budete muset jako poskytovatel **strategicky významných služeb** zavést mechanismus prověřování dodavatelského řetězce. To znamená například povinnost zjišťovat, dokumentovat a hlásit Úřadu základní informace o dodavatelích bezpečnostně významných dodávek do vymezené infrastruktury (kritické části stanoveného rozsahu) vaší společnosti.

Dopady na obce s rozšířenou působností

Obce s rozšířenou působností budou spadat do **režimu nižších povinností** poskytovatele regulované služby, kdy budou muset plnit nejméně čtyři oblasti bezpečnostních opatření – zajišťování kybernetické bezpečnosti, povinnosti vrcholného vedení, bezpečnost lidských zdrojů a řešení incidentů. Ostatní opatření se zavádějí vždy přiměřeně s ohledem na bezpečnostní potřeby uvnitř organizace.

Dopady na vysoké školy

Vysoké školy mohou být nově poskytovatelem regulované služby kvůli regulaci v odvětví **Vědy, výzkumu a vzdělávání** a odvětví **Veřejné správy**. Pokud se tedy vysoká škola věnuje oblasti výzkumu a vývoje nebo provozuje velkou výzkumnou infrastrukturu, případně provozuje službu Výkonu svěřených pravomocí, bude spadat pod jeden z režimů nového Zákona.

POSLOUCHAT

Jak se promítnou požadavky NIS2 do nového Zákona o kybernetické bezpečnosti shrnuje v podcastu TruePositive Vladěna Sasková z Národního úřadu pro kybernetickou a informační bezpečnost.

Digital Security
Progress. Protected.

Společnost ESET® již více než 30 let vyvíjí špičkový bezpečnostní software a služby, které chrání podniky, kritickou infrastrukturu a domácí uživatele na celém světě před stále sofistikovanějšími digitálními hrozbami. Vysoce výkonná a snadno ovladatelná řešení ESET nepřetržitě monitorují systémy a chrání zákazníky. ESET nabízí zabezpečení koncových a mobilních zařízení přes detekci incidentů na koncových zařízeních a reakci na ně a také šifrování a vícefaktorové ověřování. Ochrana se aktualizuje v reálném čase, takže uživatelé jsou vždy v bezpečí a podniky se nemusí obávat výpadků. Při vývoji efektivních řešení pro bezpečné používání technologií hrají zásadní roli inovace. ESET se ve svém úsilí chránit naši společnou budoucnost může opřít o výzkumná centra po celém světě. Další informace najdete na stránkách www.eset.com Můžete nás také sledovat na sociálních sítích LinkedIn, Facebook, a Twitter.

EVERSHEDS
SUTHERLAND

Eversheds Sutherland je celosvětově působící právní kancelář zabývající se také občanským právem. Má 74 poboček v 35 zemích a zaměstnává více než 3 000 právníků. Vzhledem ke svým mezinárodním zkušenostem dokáže poskytnout bezkonkurenční poradenství k problémům překračujícím národní hranice. V Evropě má společnost Eversheds Sutherland 44 poboček.

Tato příručka vznikla s podporou
divize ESET Government Affairs.