Gap analýza podle NIS2 a nového kybernetického zákona

Obsah

Úvod **2**
Cíle gap analýzy Verief **4**
Pro koho je gap analýza vhodná? 4
Otázky, na které gap analýza odpovídá 4
Předpisy, vůči kterým gap analýzu provádíme 5
Průběh gap analýzy **5**
Příprava 5
Určení dopadu regulace 6
Když zjistíme, že se vás nZKB netýká 6
Komunikace gap analýzy a úvodní školení 6
Realizace analýzy 6
Jaké od vás potřebujeme vstupy? 8
Vyhodnocení a závěrečná prezentace 9
Výstupy 9
Jak dlouho trvá gap analýza? **10**
Kolik vás bude gap analýza Verief stát? **11**
Užitečné rady **11**
Co po gap analýze? **13**
Líbí se vám náš přístup? Rádi vám s gap analýzou pomůžeme! 14

Úvod.

Česká republika má nový zákon o kybernetické bezpečnosti (nZKB), do kterého byla transponována EU směrnice NIS2. Oproti původní verzi zákona se mění okruh povinných osob i rozsah jejich povinností, na které se musí dotčené organizace v předstihu připravit.

U organizací, které už pod kybernetický zákon spadaly, nZKB nejčastěji rozšiřuje rozsah regulace, protože definuje nové typy regulovaných služeb. Zároveň se zákon nově vztahuje na tisíce dalších organizací, které se dosud otázkou souladu s tímto zákonem vůbec nemusely zabývat.

Pro ty organizace, které už kybernetickou bezpečnost do určité míry řeší, je vhodné provést gap analýzu, aby zjistily, co jim chybí k naplnění nových požadavků.

Gap analýza podle NIS2 / nZKB je analytický **nástroj**, který má pomoci organizacím zmapovat dopad nové regulace v oblasti kybernetické bezpečnosti, zjistit současný stav plnění požadavků nové regulace a bezpečnostních opatření. **Jejím cílem je identifikovat nedostatky a doporučit vhodný postup k zajištění shody s novou regulací**.

Gap analýza je užitečná zejména pro organizace, které poskytují služby v následujících odvětvích:

- Výrobní průmysl
- Digitální infrastruktura a služby
- Potravinářský průmysl
- Energetika – Elektřina, ropa a ropné produkty, plynárenství, teplárenství a vodík
- Finanční trh
- Doprava - Letecká, drážní, vodní a silniční doprava
- Chemický průmysl
- Vodní hospodářství
- Odpadové hospodářství
- Poštovní a kurýrní služby
- Vojenský průmysl
- Vesmírný průmysl

Avšak není gap analýza jako gap analýza. V Guardians.cz jsme ve spolupráci s AK Cisek připravili komplexní gap analýzu Verief, která spojuje právní jistotu s technickou odborností, což z ní dělá službu s unikátní přidanou hodnotou pro zákazníky.

Některé z benefitů gap analýzy Verief jsou:

- Nedílnou součástí výstupu je právní kvalifikace dopadu nZKB/NIS2 na vaši organizaci.
- Poskytuje jeden kvalifikovaný a ucelený výstup - jedna služba, jeden dodavatel – bez nutnosti zprostředkovávat komunikaci mezi právníky a kyberbezpečáky.
- Klíčovou částí analýzy je základní školení pro vedení organizace a garanty aktiv.
- Veškeré procesy a opatření jsou analyzovány z pohledu právních expertů i kyberbezpečnostních specialistů.
- Smlouvy s významnými dodavateli jsou posuzovány z hlediska jejich souladu s vyhláškami a metodikami NÚKIB.
- Do výstupu je zahrnuta také příprava podkladů pro registraci na Portálu NÚKIB.
- Na výstupy analýzy je možné navázat nápravnými kroky a implementací chybějících opatření s naší podporou, i bez.

V tomto materiálu vám přiblížíme, jak gap analýza Verief probíhá, jak dlouho trvá, kolik stojí a jaké konkrétní výstupy můžete očekávat.

Cíle gap analýzy Verief.

Gap analýza Verief pomáhá organizaci zacílit investice do kybernetické bezpečnosti tam, kde jsou skutečně potřeba. **Identifikuje klíčové mezery a rizika, což umožní zaměřit se pouze na relevantní řešení odpovídající byznysovým potřebám organizace. To pomáhá minimalizovat zbytečné výdaje a optimalizovat náklady. Díky Verief organizace získá jasný přehled, který jí umožní odstranit mezery v oblasti compliance a předejít tak sankcím, finančním i právním škodám a reputačním ztrátám.**

Pro koho je gap analýza vhodná?

Gap analýza Verief je ideální pro organizace, které již kybernetickou bezpečnost organizace řeší a chtějí zjistit, co jim chybí k naplnění nových požadavků.

Pokud vaše organizace doposud kybernetickou bezpečnost vůbec neřešila, je efektivnější začít s konzultací s manažerem kybernetické bezpečnosti, který vám pomůže postupně implementovat nezbytná regulační opatření. Gap analýza pro vás v takovém případě nebude přínosem.

Otázky, na které gap analýza odpovídá

Gap analýza by vám měla odpovědět na následující otázky:

- Jak na vaši organizaci dopadá NIS2 / nZKB?
- Jaké jsou přesné požadavky, které musí právě vaše organizace plnit?
- Jaký je současný stav kybernetické bezpečnosti organizace ve vztahu k nZKB?
- Jaká jsou vaše současná kyber-bezpečnostní a obchodní rizika?
- Má vaše organizace spolehlivé dodavatele a jsou s nimi správně nastavené smluvní vztahy?

- Je vaše organizace dostatečně chráněna proti právní odpovědnosti vůči zákazníkům?
- Co musíte udělat pro zajištění shody s NIS2 / nZKB?
- Kolik vás to přibližně bude stát?
- Kde může vaše organizace optimalizovat náklady a na které oblasti se naopak musí prioritně zaměřit?
- Jaké příležitosti vám NIS2 / nZKB přináší?

Předpisy, vůči kterým gap analýzu provádíme

- **Nový zákon o kybernetické bezpečnosti a jeho prováděcí právní předpisy,** zejm.:
  - Vyhláška o regulovaných službách (pomáhá nám určit, zda vaše organizace spadá pod regulaci, a pokud ano, do jakého režimu, z čehož vyplývají povinná bezpečnostní opatření, které byste následně měli aplikovat).
  - Vyhláška s bezpečnostními opatřeními pro režim nižších povinností.
  - Vyhláška s bezpečnostními opatřeními pro režim vyšších povinností.
- **Prováděcí nařízení EU ke směrnici NIS2 pro vybrané typy digitálních služeb** Prováděcí nařízení - EU - 2024/2690 - EN - EUR-Lex.

Oficiální informace k těmto předpisům naleznete na webu regulátora (NÚKIB), na Portálu NÚKIB.

Průběh gap analýzy.

Příprava

Přípravná fáze zahrnuje sběr podkladů (vstupů) od zástupců vaší organizace a plánování (tvorba harmonogramu) jednotlivých analytických činností se zástupci organizace. Pro

zefektivnění procesu analýzy provádíme sběr podkladů pomocí specializovaných nástrojů.

Určení dopadu regulace

Tato fáze spočívá ve vytvoření mapy služeb a v posouzení, zda organizace spadá pod nZKB. Součástí posouzení je i zohlednění vlastnické struktury u holdingů, propojených podniků atp.

Když zjistíme, že se vás nZKB netýká

Může se stát, že po prvotní analýze vstupních podkladů zjistíme, že na vaši organizaci nový kybernetický zákon nedopadá. V takovém případě naše analýza končí předáním právního posouzení dopadu regulace a vyrovnáním dosud provedených prací.

Komunikace gap analýzy a úvodní školení

Pro efektivní průběh gap analýzy zpravidla organizujeme úvodní školení / prezentaci pro relevantní zástupce vaší organizace (nejčastěji statutární zástupce, top management a klíčové garanty aktiv), kde vysvětlíme požadavky nové regulace, cíl gap analýzy, její průběh i rozsah potřebné součinnosti.

Realizace analýzy

Na přípravnou fázi navazuje samotná realizace analýzy. Ta zahrnuje analýzu vstupních dat, případný dodatečný sběr dat a rozhovory s jednotlivými zástupci organizace. Těmi jsou zpravidla:

- zástupci vedení organizace,
- garanti aktiv,
- oddělení bezpečnosti,
- ICT / OT pracovníci,
- zástupci HR,
- právní oddělení,
- compliance oddělení,
- DPO,
- nákupní oddělení,
- zástupci klíčových dodavatelů.

***Garant aktiva** = bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva. Klíčové je zmínit, že téměř každá organizace má osoby, které tuto roli fakticky zastávají, i když nemusí být formálně označeny jako garanti aktiv.*
Zpravidla jimi jsou zástupci vrcholného vedení, vedoucí pracovníci (např. odpovědní pracovníci za určité týmy, agendy atp.) nebo osoby odpovědné za určité technologie. Garanti aktiv jsou naprosto klíčoví při mapování aktiv organizace, při řízení aktiv obecně a při řízení rizik. Zároveň pomáhají, mimo jiné, zajistit, aby bezpečnostní opatření byla implementována v souladu s obchodními/provozními potřebami organizace a aby podporovala její strategické cíle.

Klíčové činnosti garanta aktiva jsou zejm.:

- *Odpovědnost za zajištění rozvoje, použití a bezpečnosti aktiva.*
- *Spolupráce s ostatními osobami zastávajícími bezpečnostní role.*
- *Provádění určování a hodnocení aktiv a rizik.*

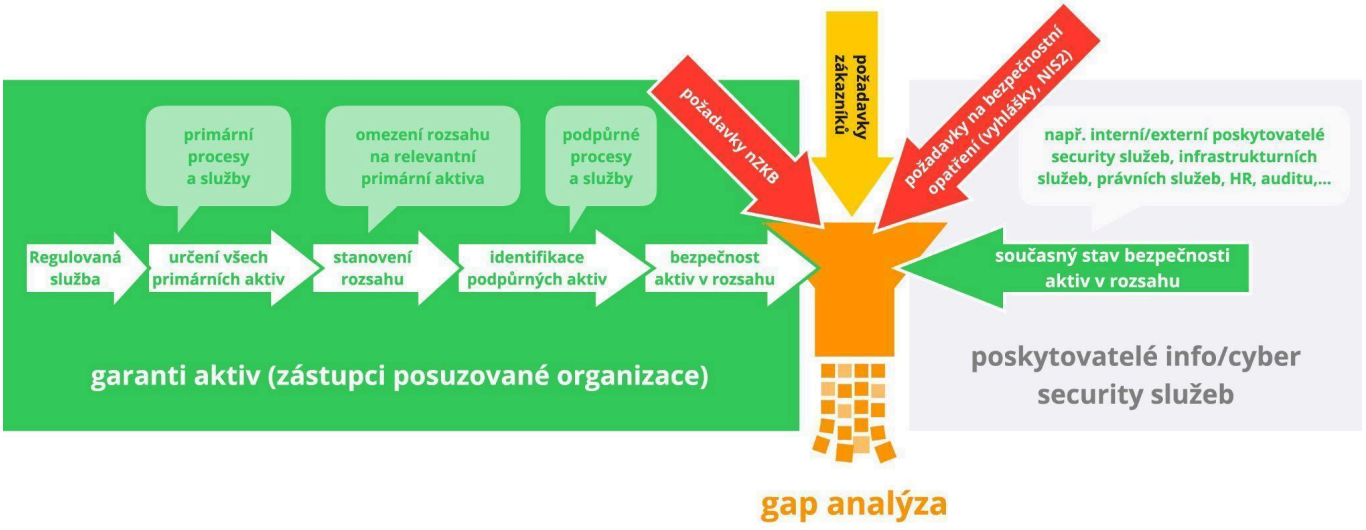
***ICT** = Informační a komunikační technologie.*

***OT** (Operational Technology) = Provozní technologie (zařadit sem můžeme např. průmyslové a řidicí systémy, SCADA systémy apod.).*

Průběh analýzy je možné rozdělit do dvou základních logických celků:

- **„Businessový"**
  - Zahrnuje schůzky analytického týmu s garanty aktiv jejichž cílem je určit rozsah podle nZKB, identifikovat garanty pro aktiva v tomto rozsahu a zjistit, kdo v organizaci odpovídá za relevantní bezpečnostní opatření.
- **Odborný (z hlediska kyber-bezpečnostních požadavků)**
  - Spočívá ve schůzkách analytického týmu se zástupci interních poskytovatelů relevantních bezpečnostních opatření (např. s odděleními

zajišťujícími fyzickou bezpečnost, procesy nákupu (řízení dodavatelů), síťovou bezpečnost, atd.). Společně s nimi detailně procházíme, jak jsou opatření ve skutečnosti plněna a identifikujeme případné nedostatky ve vztahu k požadavkům regulace.



Jaké od vás potřebujeme vstupy?

Abychom mohli provést analýzu současného stavu, budeme od vás potřebovat tyto informace:

- Základní údaje o organizaci (název, IČ apod.), přehled o organizační struktuře a počtu zaměstnanců.
- Role a odpovědnosti (organizační řád, plné moci, pověření k jednání s NÚKIB/CSIRT).
- Seznam relevantních zástupců organizace vč. kontaktních údajů.
- Seznam aktiv (jaké jsou vaše klíčové procesy a služby a jejich závislostí na podpůrných procesech a službách).
- Přehled ICT / OT a bezpečnostních služeb v organizaci (+ bezpečnostních nástrojů, případně i dodavatelů klíčových služeb).

- Smlouvy s klíčovými dodavateli ICT/OT a cloudových služeb (včetně příloh SLA a bezpečnostních požadavků).
- Případný přehled relevantních kyber-bezpečnostních požadavků vašich zákazníků nebo jiných regulací.
- Doložky o bezpečnosti v rámcových smlouvách, objednávkách a SOW (auditní práva, oznamovací povinnosti, sankce za porušení bezpečnostních povinností, atp.).
- Bezpečnostní dokumentace (směrnice, politiky, bezpečnostní dokumentace).
- Informace o bezpečnostních procesech.
- Informace o využívaných bezpečnostních nástrojích vč. výstupů z těchto nástrojů (reporty, skeny zranitelností, exporty, apod.)
- Záznamy o bezpečnostních incidentech a „near-misses“ (pro validaci povinností hlášení) vč. incident response plánů / incident playbooků.
- Podklady z jakýchkoliv dříve vedených řízení před ÚOOÚ nebo NÚKIB.
- Informace z předešlých penetračních testů a auditů kybernetické bezpečnosti.
- Informace o relevantních standardech, které máte zavedeny, případně i certifikovány (např. ISO/IEC 27001, ISO 22 301).
- Další relevantní informace ve vztahu k řízení kybernetické bezpečnosti.

Vyhodnocení a závěrečná prezentace

Cílem vyhodnocení je propojit jednotlivé výstupy sběru dat, správně je analyzovat a interpretovat jejich výsledky. Výsledky jsou následně promítnuty do závěrečné zprávy a prezentovány vedení organizace i garantům aktiv.

Výstupy

- Právní mapa povinností a checklist registrace na Portálu NÚKIB.
- Identifikace primárních a podpůrných aktiv (příprava pro identifikaci rozsahu podle nZKB).

- Zmapování současného stavu plnění bezpečnostních opatření.
- Závěrečná zpráva s doporučeními a manažerským shrnutím.
    - Výstupem analýzy je závěrečná zpráva obsahující identifikované nedostatky vztažené ke kritériím, které vychází z požadavků kybernetického zákona a souvisejících prováděcích právních předpisů.
- Seznam relevantních scénářů rizik, vč. přehledu sankčních rizik.
- Akční plán s doporučenými nápravnými opatřeními k dosažení souladu, včetně návrhu prioritizace, časování jednotlivých aktivit / implementace jednotlivých opatření.
- Notifikační playbook incidentů.
- Governance balíček (návrh rozhodnutí vedení o přidělení odpovědností, směrnice ke školení managementu atp.).
- Smluvní balíček (např. vzorové bezpečnostní a SLA doložky pro dodavatele).
- Odhad finančních nákladů na zavedení a údržbu jednotlivých identifikovaných chybějících opatření.
- Odhad množství ostatních zdrojů, včetně lidských zdrojů, potřebných na zavedení a údržbu jednotlivých identifikovaných chybějících opatření.
- Osobní prezentace výstupů zástupcům organizace.

Jak dlouho trvá gap analýza?

Provedení gap analýzy v rozsahu, jaký popisuje náš whitepaper se pohybuje **u malých a středních podniků** okolo **1-3 měsíců.** Ve **velkých podnicích a korporátech** může **trvat déle. Termín dokončení se odvíjí zejména od počtu regulovaných služeb a od režimu regulace, který určuje rozsah posuzovaných bezpečnostních opatření (režim nižších povinností, vyšších povinností, požadavky pro vybrané digitální služby podle prováděcího aktu k NIS2). Významný vliv má také dostupnost zástupců na straně organizace, kteří musí poskytnout vstupní informace a součinnost při provádění analýzy.**

Kolik vás bude gap analýza Verief stát?

Typově se gap analýza Verief pohybuje cenově v těchto úrovních:

Organizace zavádějící požadavky...	Gap analýza s právním posouzením
... jen podle vyhlášky pro nižší režim regulace	do (<) 200.000 Kč
... jen podle vyhlášky pro vyšší režim regulace	do (<) 300.000 Kč
... jen podle prováděcího nařízení EU k NIS2 pro digitální služby	do (<) 300.000 Kč
... podle prováděcího nařízení EU k NIS2 pro digitální služby u některých regulovaných služeb a současně požadavky podle vyhlášky pro vyšší režim regulace u ostatních regulovaných služeb	od (>) 250.000 Kč

Užitečné rady.

- Pro úspěšnou realizaci gap analýzy je nutné počítat se součinností v podobě poskytování informací a alokace potřebných časových kapacit ze strany zainteresovaných osob (vrcholné vedení organizace, bezpečnostní role, garanti aktiv apod.) a v některých případech i na straně významných dodavatelů. U holdingů je například nezbytná i součinnost „kompetenčního" centra, které poskytuje služby kybernetické bezpečnosti.

- Při výběru dodavatele gap analýzy se zaměřte na prokazatelné zkušenosti týmu, který analýzu provádí.
- Pokud si nejste jisti, jaké budou vaše regulované služby, doporučujeme zvolit analýzu Verief Verief, která vám poskytne i nezbytné právní posouzení dopadu a mnohem více.
- Kvalitní gap analýza není o 1-2 MDs práce a zaškrtaném checklistu.
- Pokud se v rámci gap analýzy rovnou zaměříte na plnění požadovaných bezpečnostních opatření, bez předchozí identifikace aktiv, bude vám chybět potřebný kontext a výsledky analýzy budou příliš obecné.
- Z analýzy není dobré vynechat business vlastníky klíčových procesů a služeb (garanty aktiv). Jejich absence může způsobit, že analýza nebude provedena na základě správných nebo úplných informací.
- Gap analýzu není ekonomicky rozumné provádět, pokud s kyberbezpečností začínáte zcela „na zelené louce“. V takové situaci je lepší rovnou zapojit expertní firmu (jako je např. Guardians.cz), která vám pomůže se zajištěním souladu s novou regulací.
- Výstupy gap analýzy poskytují rámcový obraz o stavu vaší organizace a doporučení k dalším krokům. Jejím předmětem není navrhovat konkrétní technologie ani stanovit jejich přesné nacenění. Tyto kroky navazují až v rámci implementačních projektů nebo PoC k jednotlivým technologiím, jejichž cílem je zajistit splnění požadavků regulace.

Co po gap analýze?

Na gap analýzu Verief je vhodné navázat zahájením projektu, jehož cílem je dosažení souladu s relevantními požadavky regulace. Prakticky to znamená implementaci chybějících bezpečnostních opatření, odstranění zjištěných nedostatků a realizaci případných doporučení (úpravu procesů a smluv, výběr vhodných nástrojů atp.). Projekt tak plynule navazuje na výstupy z gap analýzy.

S realizací tohoto projektu vám za Verief tým, složený z expertů z Guardians.cz a AK Cisek, velice rádi pomůžeme. Věříme, že s námi budete spokojeni natolik, že navážete i na naše další služby služby manažera kybernetické bezpečnosti od Guardians.cz, nebo služby Managed Compliance od AK Cisek, která obsahuje např. průběžné právní poradenství, aktualizace směrnic a smluv, školení managementu, podporu při kontrolách NÚKIB a komunikaci s CSIRT/GovCERT.

Líbí se vám náš přístup? Rádi vám s gap analýzou pomůžeme!

Guardians.cz je tým zkušených odborníků v oblasti řízení informační a kybernetické bezpečnosti. Specializujeme se na systém řízení bezpečnosti informací podle ISO/IEC 27001 a navazujících norem, kybernetický zákon a management bezpečnosti AI. Poskytujeme služby manažera kybernetické bezpečnosti, auditora kybernetické bezpečnosti a pracujeme s řadou moderních technologií, které pomáháme implementovat u našich zákazníků. Přestože jsme mladá firma, seniorní členové našeho týmu mají mnohaleté prokazatelné zkušenosti. Poskytování služeb v oblasti kybernetické bezpečnosti a poskytování služeb manažera kybernetické bezpečnosti máme certifikované podle ČSN EN ISO/IEC 27001:2023. Při spolupráci s našimi klienty usilujeme o to, aby byla kybernetická bezpečnost jejich organizací řízená smysluplně.

Věřím, že s případnou spoluprací s naším týmem budete spokojeni.

S úctou,

Ing. Martin Konečný, MBA, CISM
martin.konecny@guardians.cz
+ 420 736 709 865

Advokátní kancelář Císek je tým právníků, kteří propojují právo, technologie a byznys. Máme hluboké znalosti v právu informačních technologií, právu duševního vlastnictví a kybernetické bezpečnosti. Specializujeme se proto hlavně na podporu podniků, které inovují a zajímají se o digitální řešení. Naše řešení se soustředí nejen na soulad s regulací, ale také na praktickou ochranu vašich dat a kontinuitu podnikání.

S úctou,

Mgr. Jiří Císek, LL.M.

jiri@akcisek.cz

Máte zájem o gap analýzu nebo konzultaci?

Stačí se obrátit na jednoho z nás.