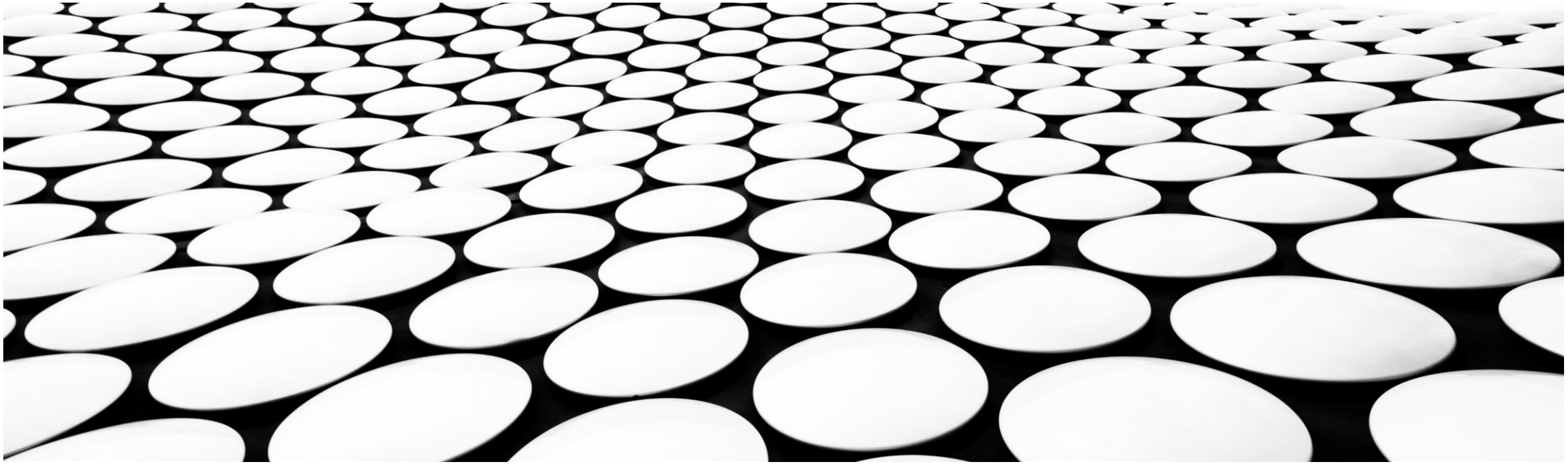
NIS2 A DORA:
(R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI?

JIŘÍ DIEPOLT

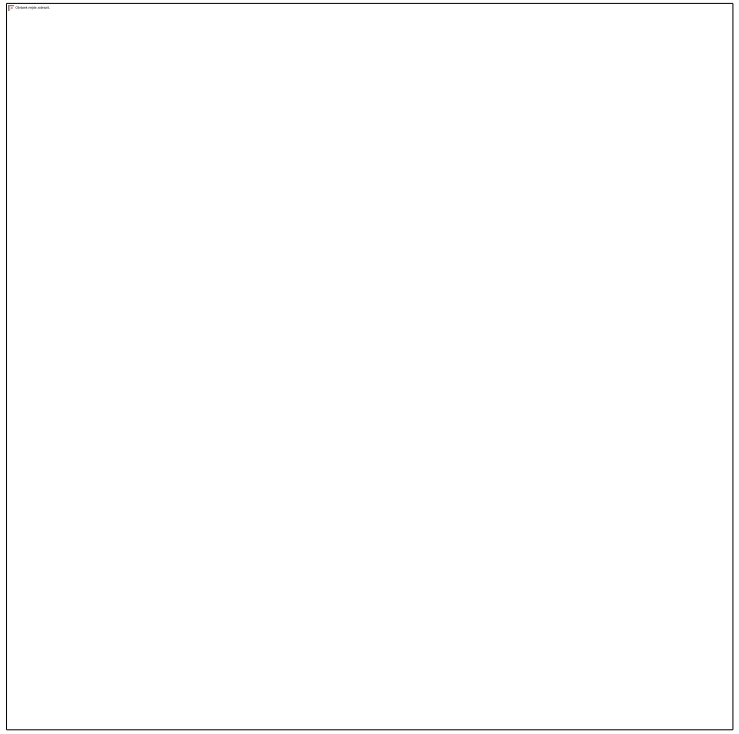
LISTOPAD 2024



DORA & NIS2
(R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI

Agenda

- Úvod
- Požadavky na audit
- Predikce hrozeb a rizik kyberbezpečnosti
- Audit kybernetické bezpečnosti
  - Typické problémy
  - Nejčastější zjištění
  - Využití AI/LLM
- Závěr



DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI?
ÚVOD

Linkedin

CV

Popis

Typický obrázek velikosti A4 (pokud je dobře promyšlený a vizuálně informativní) by mohl "vydat" přibližně 500 až 1 000 slov.

Disclaimer: Skutečný informační obsah konkrétního obrázku může být výrazně nižší nebo vyšší ☺sv závislosti na jeho složitosti, detailnosti a typu zobrazovaných informací. Toto číslo by mělo být bráno jako orientační hodnota, nikoli jako přesné měření.

https://www.linkedin.com/in/jiri-diepolt/

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011

Účinnost nařízení DORA – 17. 1. 2025

Návrh nového zákona a vyhlášky o kybernetické bezpečnosti připravil NÚKIB

25.07.2024	Návrh byl předložen Poslanecké sněmovně
17.09.2024	Proběhlo 1. čtení, přikázáno výborům a komisím

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI?

- **Investiční podniky**: společnosti poskytující investiční služby
- **Poskytovatelé služeb souvisejících s kryptoaktivy:** společnosti nabízející služby v oblasti kryptoměn
- **Platební instituce a instituce elektronických peněz:** subjekty zajišťující platební služby a vydávání elektronických peněz
- **Obchodníci s cennými papíry**: společnosti obchodující s cennými papíry
- **Správci alternativních investičních fondů:** subjekty spravující alternativní investiční fondy
- **Pojišťovny a zajišťovny:** subjekty nabízející pojišťovací a zajišťovací služby
- **Úvěrové instituce:** banky a spořitelny
- **Poskytovatelé služeb IKT:** dodavatelé informačních a komunikačních technologií pro výše uvedené finanční instituce

přibližně 600 společností v ČR

přibližně 6000 společností v ČR

NIS2 Directive

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI?

Oblasti

- Rámec **řízení rizik v oblasti IKT**
- **Řízení incidentů** souvisejících s IKT
- **Testování digitální** provozní odolnosti
- Řízení IKT rizik spojených s **třetími stranami**

Dokumentace

Název dokumentu nebo části dokumentu
Zpráva o přezkumu rámce pro řízení rizika v oblasti IKT (D)
Strategie digitální provozní odolnosti (D)
Strategie více dodavatelů IKT (D/Č s 2)
Dokumentace aktiv vůči podporovanm funkcím (D)
Katalog rizik (D/Č s 4)
Konfigurační DB aktiv (D/Č s 4)
Procesy podporované dodavateli IKT (D/Č s 4)
Politika zabezpečení informací (D)
Architekura, postupy a protokoly řízení sítí a infrastruktury (D)
Politika a postupy fyzické a logické bezpečnosti (D)
Politika a protokoly pro silné ověřovací mechanismy (D)
Politika a postupy pro řízení změn IKT (D)
Politka pro dočasné opravy a aktualizace (D)
Popis postupů včasné detekce neobvyklých aktivit (D/Č s 8)
Politika zachování provozu IKT (D)
Plány a reakce obnovy (D/Č s 15)
Plány na zachování provozu (D/Č s 15)
Analýza dopadu na činnost (D)
Záznamy činnosti před výpadky o během výpadků po aktivaci plánů (D)
Odhad souhrnných ročních nákladů IKT incidentů (D)
Politika a postupy zálohování (D/Č s 15)
Postupy a metody obnovy (Č s 21)
Programy zvyšování povědomí o bezpečnosti v oblasti IKT a školení o digitální provozní odolnosti (D)
Krizové komunikační plány (D/Č s 25)
Komunikační politika pro interní zaměstnance a externí zainteresované strany (D)
Postupy pro zajištění bezpečnosti údajů a systémů (D)
Postupy řízení kapacity a výkonu (D)
Postupy řízení zranitelností (D)
Postupy pro vedení protokolů (D)
Politika, postupy a protokoly na ochranu informací během přenosu (D)
Politika pro řízení projektů v oblasti IKT (D)
Politika upravující pořizování, vývoj a údržbu systému IKT (D)
Politika fyzické a environmentální bezpečnosti (D)
Politika a postupy správy identit (D)
Politika správy přístupů (D)
Politika a postupy řízení IKT incidentů; pro subjekty platebního styku včetně řízení provozních a bezpečn
Záznamy veškerých incidentů souvisejících s IKT a závažné kybernetické hrozby (D)
Postupy pro konzistentní a integrované sledování, řešení a následná opatření pro incidenty související s
Postupy klasifikace IKT incidentů a kybernetických hrozeb (D)
Program a postupy testování digitální provozní odolnosti (D)
Postupy pro stanovení priorit, klasifikaci a nápravu všech problémů zjištěných při provádění testů (D/Č s
Metodiky ověřování, zda všechny slabiny nedostatky či vady odhaleny (D/Č s 40)
TLPT: rámec TIBER-EU (v gesci Sekce dohledu nad finančním trhem II zatím nikdo, ale jako součást kon
Strategie/politika pro riziko v oblasti IKT spojené s třetími stranami (D/Č s 3)
Registr ujednání s třetími stranami v oblasti IKT (D)
Strategie a plány ukončení smluvního vztahu (D/C)
Plány přechodu k alternativnímu poskytovateli (D/C)

Organizační opatření

§4 Systém řízení bezpečnosti informací

§5 Povinnosti vrcholného vedení

§6 Bezpečnostní role

§7 Řízení bezpečnostní politiky a bezpečnostní dokumentace

§8 Řízení aktiv

§9 Řízení rizik

§10 Řízení dodavatelů

§11 Bezpečnost lidských zdrojů

§12 Řízení změn

§13 Akvizice, vývoj a údržba

§14 Řízení přístupu

§15 Zvládání kybernetických bezpečnostních událostí a incidentů

§16 Řízení kontinuity činností

§17 Audit kybernetické bezpečnosti

Technická opatření

§ 18 Fyzická bezpečnost

§ 19 Bezpečnost komunikačních sítí

§ 20 Správa a ověřování identit

§ 21 Řízení přístupových oprávnění

§ 22 Detekce kybernetických bezpečnostních událostí

§ 23 Zaznamenávání událostí

§ 24 Vyhodnocování kybernetických bezpečnostních událostí

§ 25 Aplikační bezpečnost

§ 26 Kryptografické algoritmy

§ 27 Zajišťování dostupnosti regulované služby

§ 28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI? POŽADAVEK NA OVĚŘENÍ & AUDIT - I

- **Vedoucí orgán schvaluje** a pravidelně přezkoumává **plány interních auditů IKT**, které finanční subjekt vypracovává, **audity IKT** a jejich podstatné změny.
- Finanční subjekty zajistí náležité oddělení a **nezávislost** vedoucích funkcí, kontrolních funkcí a **interních auditních funkcí**,
- Rámec pro řízení rizika v oblasti IKT se zdokumentuje a reviduje alespoň jednou ročně nebo pravidelně v případě mikropodniků a rovněž po výskytu závažného incidentu souvisejícího s IKT a na základě pokynů dohledu nebo závěrů vyvozených na základě příslušných **testů či auditů digitální provozní odolnosti**.

<u>Auditor kybernetické bezpečnosti</u>

a) je bezpečnostní role odpovědná za provádění auditu kybernetické bezpečnosti,

přičemž výkonem této role může být pověřena osoba, která je pro tuto činnost vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací

1. po dobu nejméně tří let, nebo

2. po dobu jednoho roku, pokud absolvovala studium na vysoké škole,

b) zaručuje, že **provedení auditu** kybernetické bezpečnosti **je nestranné** a

c) **nesmí být pověřen výkonem jiných bezpečnostních rolí.**

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI? POŽADAVEK NA OVĚŘENÍ & AUDIT - II

- **Finanční subjekty musí zajistit**, aby jejich **rámec pro řízení rizik ICT byl pravidelně kontrolován** nezávislými interními nebo externími auditory.
- **Pokročilé testování odolnosti**, včetně penetračních testů, musí být prováděno nezávislými testery, a to buď interními nebo externími, což zaručuje objektivitu výsledků a validaci kybernetické odolnosti.
- **Kritičtí poskytovatelé ICT** služeb musí podléhat nezávislému auditu alespoň jednou ročně, což má zajistit soulad s regulatorními požadavky a řízením rizik spojených se závislostí na externích poskytovatelích.
- **Dohledový orgán může pověřit nezávislé auditory** nebo experty prováděním šetření nebo hodnocení ICT rizik a kontroly v kritických oblastech, což podporuje nestranné posouzení rizik.

NIS2 Directive

§ 17

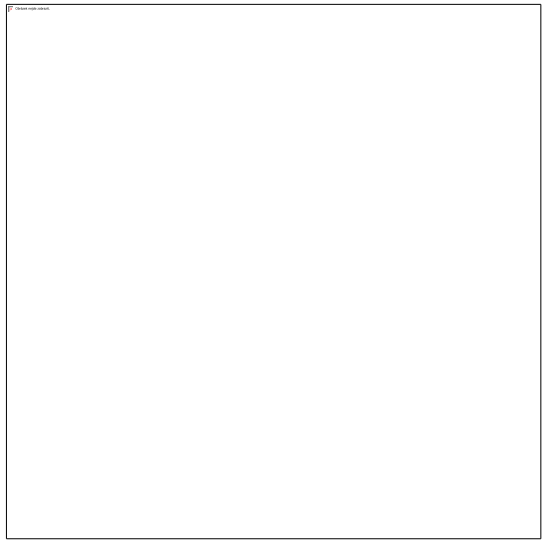
Provádění auditu kybernetické bezpečnosti

(1) Povinná osoba stanoví plán provádění auditu kybernetické bezpečnosti.
(2) Povinná osoba v rámci auditu kybernetické bezpečnosti
a) posuzuje zda byla zavedena bezpečnostní opatření požadovaná zákonem a touto vyhláškou,
b) posuzuje soulad zavedených bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy, smluvními závazky a nejlepší praxí a
c) provádí a dokumentuje audit dodržování pravidel a postupů stanovených v bezpečnostní politice, včetně přezkoumání technické shody a dříve stanovených nápravných opatření podle odstavce 4.
(3) Povinná osoba zohlední výsledky auditu kybernetické bezpečnosti podle odstavce 2 v
a) plánu zvládání rizik,
b) prohlášení o aplikovatelnosti a
c) plánu rozvoje bezpečnostního povědomí.
(4) Povinná osoba stanoví případná nápravná opatření pro splnění požadavků podle odstavce 2.
(5) Audit kybernetické bezpečnosti podle odstavce 2 je prováděn
a) při významných změnách, v rámci jejich rozsahu,
b) v pravidelných intervalech alespoň po dvou letech a
c) v souladu s plánem auditu kybernetické bezpečnosti.
(6) Není-li v odůvodněných případech možné provést audit v intervalu podle odstavce 5 písmene b) v celém rozsahu podle odstavce 2, je možné audit kybernetické bezpečnosti provádět průběžně po systematických celcích. V takovém případě je nutno audit v celém rozsahu podle odstavce 2 provést nejpozději do pěti let.
(7) Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanoveným v § 6 odst. 4, která nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI? PŘEDPOVĚDI HROZEB KYBERNETICKÉ BEZPEČNOSTI PRO ROK 2025

Předpovědi dle CHECKPOINT

- **Ransomware** se zdokonalí **pomocí AI**, očekávají se 2-3 velké útoky na dodavatelské řetězce
- **AI posílí kyberútoky** - dokonalejší phishing, **automatizované útoky**, adaptivní malware
- Vzroste riziko úniku dat kvůli nesprávnému **používání AI** nástrojů ve firmách
- Bezpečnostní centra začnou využívat **AI "co-piloty"** pro lepší detekci a reakci na hrozby
- **Kvantové počítače** začnou ohrožovat současné šifrovací metody
- **Sociální sítě** se stanou hlavním zdrojem útoků díky **deepfake** technologiím
- Role **CISO** se bude více **propojovat s CIO**, důraz na balancování bezpečnosti a inovací
- **Cloud bezpečnost** se zaměří na prevenci místo reakce na incidenty
- Prohloubí se **nedostatek odborníků** na kybernetickou bezpečnost
- **Zpřísní se regulace (DORA, NIS2) a podmínky kybernetického pojištění**



DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI?

RIZIKA AI

Doména
1. Diskriminace a toxicita
2. Soukromí a bezpečnost
3. Dezinformace
4. „Zlovolní“ aktéři
5. Interakce člověk-počítač
6. Socioekonomické a environmentální
7. Bezpečnost, selhání a omezení AI systémů

Doména	Subdoména	Popis
3 Dezinformace (neúmyslné)	**3.1 Falešné nebo zavádějící informace**	AI systémy, které **neúmyslně generují nebo šíří nesprávné nebo klamné informace**, což může vést k nepřesným přesvědčením u uživatelů a oslabit jejich autonomii. Lidé, kteří činí **rozhodnutí na základě falešných přesvědčení**, mohou zažít fyzickou, emocionální nebo materiální újmu.
	3.2 Znečištění informačního ekosystému a ztráta společné reality	**Vysoce personalizovaná dezinformace generovaná AI vytvářející „filtrační bubliny“**, kde jednotlivci vidí pouze to, co odpovídá jejich stávajícím přesvědčením, čímž podkopávají sdílenou realitu, oslabují sociální soudržnost a politické procesy. **Kontaminace dat v LLM modelech**, viz např. https://www.unite.ai/cs/the-hidden-influence-of-data-contamination-on-large-language-models/
4 Zlovolní aktéři (úmyslné)	**4.1 Dezinformace, sledování a ovlivňování ve velkém měřítku**	Používání AI systémů k provádění **dezinformačních kampaní, škodlivého sledování nebo cílené a sofistikované automatizované cenzury a propagandy** s cílem **manipulovat** veřejným míněním.
	4.2 Kybernetické útoky, vývoj nebo použití zbraní, a masové škody	Použití AI systémů **k vývoji kybernetických zbraní** (např. kódování levnějšího, účinnějšího malwaru), vývoj nových nebo vylepšení stávajících zbraní (např. smrtících autonomních zbraní), nebo použití zbraní k způsobení masové újmy.
	4.3 Podvody a cílená manipulace	Použití AI systémů k **získání osobní výhody nad ostatními**, například prostřednictvím podvodů, vydírání nebo cílené manipulace s přesvědčeními nebo chováním. Příklady zahrnují **AI-facilitované plagiátorství pro výzkum nebo vzdělávání**, **vydávání se za důvěryhodnou nebo falešnou osobu** za účelem nelegitimního finančního zisku nebo vytváření ponižujícího nebo sexuálního zobrazování.

https://airisk.mit.edu/#Causal-Taxonomy-of-AI-Risks

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI? TYPICKÉ PROBLÉMY PŘI PROVÁDĚNÍ AUDITU KYBERNETICKÉ BEZPEČNOSTI

- **Nedostatek a kvalita zdrojů (auditorů):** Nutnost ICT a kyber specializace dle DORA/NIS2Povinné kontinuální vzdělávání v nových technologiích. Požadavek na certifikace a prokazatelné kompetence.
- **Nepravidelnost a nedostatečných rozsah auditů a kontrol**
- **Neefektivní řešení zjištěných nedostatků:** Po identifikaci problémů během auditu musí organizace najít efektivní způsob, jak tyto problémy řešit. Dokumentované nápravné plány s termíny, reporting managementu.
- **Komplexnost a rozsah bezpečnostních opatření:** Audit musí zjistit, zda byla implementována všechna legislativně požadovaná opatření.
- **Posuzování souladu s mnoha různými předpisy:** Audit musí posoudit shodu nejen s právními předpisy, ale také s interními směrnicemi, smluvními závazky a nejlepšími praxemi.
- **Ověřování nových oblasti (není zatím praktická zkušenost) -** testování digitální odolnosti, Third-party risk management, …

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI? TYPICKÁ ZJIŠTĚNÍ V RÁMCI AUDITU KYBERNETICKÉ BEZPEČNOSTI

- **Řízení rizik:** Nedostatečná identifikace a hodnocení kybernetických rizik, absence aktualizací a reakce na nové hrozby, AR je pouze formální, ….
- **Řízení přístupových práv**: Nepravidelné revize přístupových práv, nadměrná oprávnění, absence principu minimálních práv.
- **Ochrana kritických systémů:** Nedostatečná ochrana před kybernetickými útoky, zranitelnosti v kritických systémech a aplikacích (hardening, patchování, sledování zranitelnost, …)
- **Incident management:** Absence nebo neaktuální plány pro reakci na bezpečnostní incidenty, nedostatečný monitoring a hlášení incidentů.
- **Kontinuita podnikání a obnova po havárii:** Chybějící nebo neaktualizované plány kontinuity a obnovy IT systémů, nedostatek pravidelného testování.
- **Ochrana dat a šifrování:** Slabá nebo nekompletní opatření pro ochranu dat, nedostatečné šifrování citlivých informací.
- **Dodavatelské riziko a třetí strany:** Neadekvátní správa a kontrola dodavatelů a třetích stran, které mohou představovat bezpečnostní rizika.
- **Zaměstnanecké školení a bezpečnostní povědomí:** Nedostatek pravidelného školení a osvěty zaměstnanců o kybernetických hrozbách a bezpečnostních postupech.

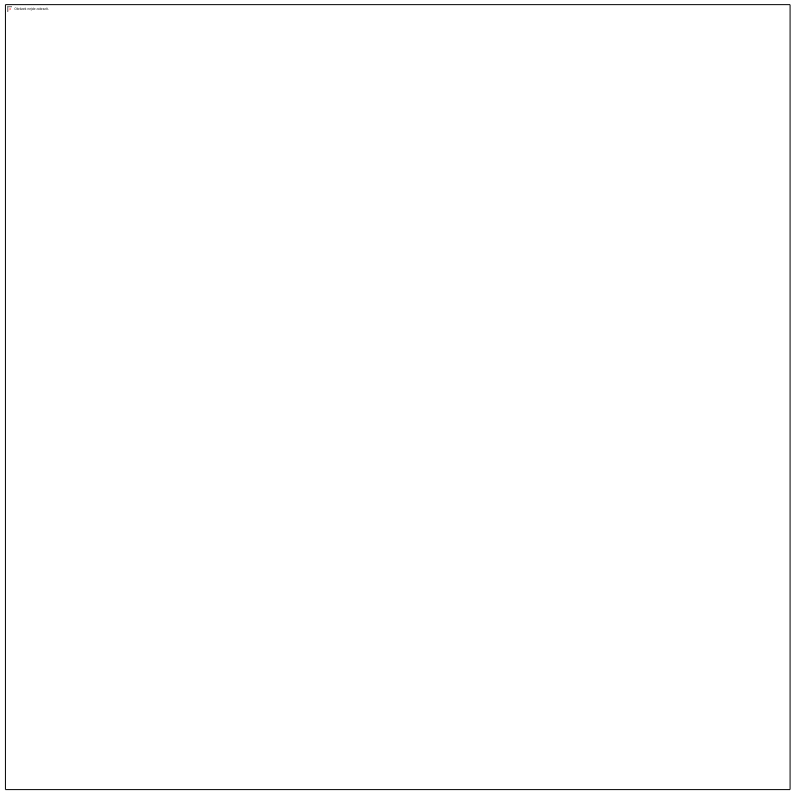
DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI? MOŽNOSTI VYUŽITÍ AI/LLM V RÁMCI AUDITU

Možnosti užití AI	Rizika užití AI	Možná řešení
• **Analýza dokumentace** (AI může rychle procházet velké množství dokumentů, politiky a směrnice a identifikovat nesoulady s požadavky DORA/NIS2) • **Reporting** (generování auditních zpráv, sledování nápravných opatření, příprava podkladů pro regulátora) • **Zhodnocení rizik** (AI může pomoci s identifikací a kvantifikací rizik, včetně analýzy vztahů mezi různými rizikovými faktory) • **Revize přístupových práv** (LLM mohou provádět pravidelné revize přístupových práv, identifikovat nadměrná oprávnění nebo nepřiměřená práva a doporučit změny v souladu s principem minimálního oprávnění) • **Analýza incidentů** (zpracování hlášení o bezpečnostních incidentech, identifikace vzorců a trendů, predikce potenciálních hrozeb)	• **Kvalita dat** (AI závisí na kvalitě vstupních dat - hrozí zkreslené nebo nesprávné závěry kvůli nekompletním nebo nepřesným datům) • **Validace výstupů** (obtížné ověření správnosti AI analýz a doporučení, riziko falešně pozitivních nebo falešně negativních nálezů) • **Bezpečnost AI nástrojů/dat** (riziko úniku citlivých dat při používání externích AI služeb, nutnost zajištění bezpečného prostředí) • **Přílišná závislost** (riziko ztráty kritického myšlení auditorů a přehlédnutí problémů, které AI neodhalí) • **Technická komplexita** (obtížné nastavení a údržba AI systémů, závislost na specifických technických znalostech) • **Lidský faktor** (nedostatečné pochopení limitů AI, přeceňování schopností AI, nesprávná interpretace výsledků)	• On-premise řešení (využití AI systémů instalovaných lokálně v zabezpečeném prostředí organizace) • Anonymizace dat (odstranění citlivých informací před zpracováním AI) • Vlastní AI modely (vývoj a trénování vlastních AI modelů na interních datech) • Omezené využití (použití AI pouze pro předběžnou analýzu nebo méně citlivé dokumenty

DORA & NIS2 - (R)EVOLUCE V AUDITU A KYBERNETICKÉ BEZPEČNOSTI? SHRNUTÍ

DORA & NIS2 v auditu a kybernetické bezpečnosti

- **Posílené požadavky na řízení ICT rizik**
  DORA a NIS2 definují strukturovaný přístup k řízení ICT rizik, zahrnující auditní a kontrolní mechanismy na podporu kybernetické odolnosti.
- **Nezávislý audit a testování odolnosti**
  Finanční subjekty musí pravidelně provádět nezávislé audity a pokročilé testování digitální provozní odolnosti (včetně penetračních testů),
- **Důraz na kontrolu třetích stran**
  Kritičtí poskytovatelé ICT služeb podléhají každoročnímu posouzení, auditu a vyhodnocení s cílem minimalizovat rizika spojená s třetími stranami.
- **Komplexní rámec pro řízení incidentů**
  DORA zavádí harmonizované procesy pro řízení (včetně hlášení kritických) incidentů, které jsou integrovány s predikcí hrozeb a kontinuálním monitorováním.
- **Budoucí vývoj a predikce**
  Rostoucí význam AI v oblasti kybernetické bezpečnosti a řízení rizik může výrazně změnit podobu detekce hrozeb a zranitelností, jakož i auditu.



Dotazy & komentáře na jiri.diepolt@rvda.cz