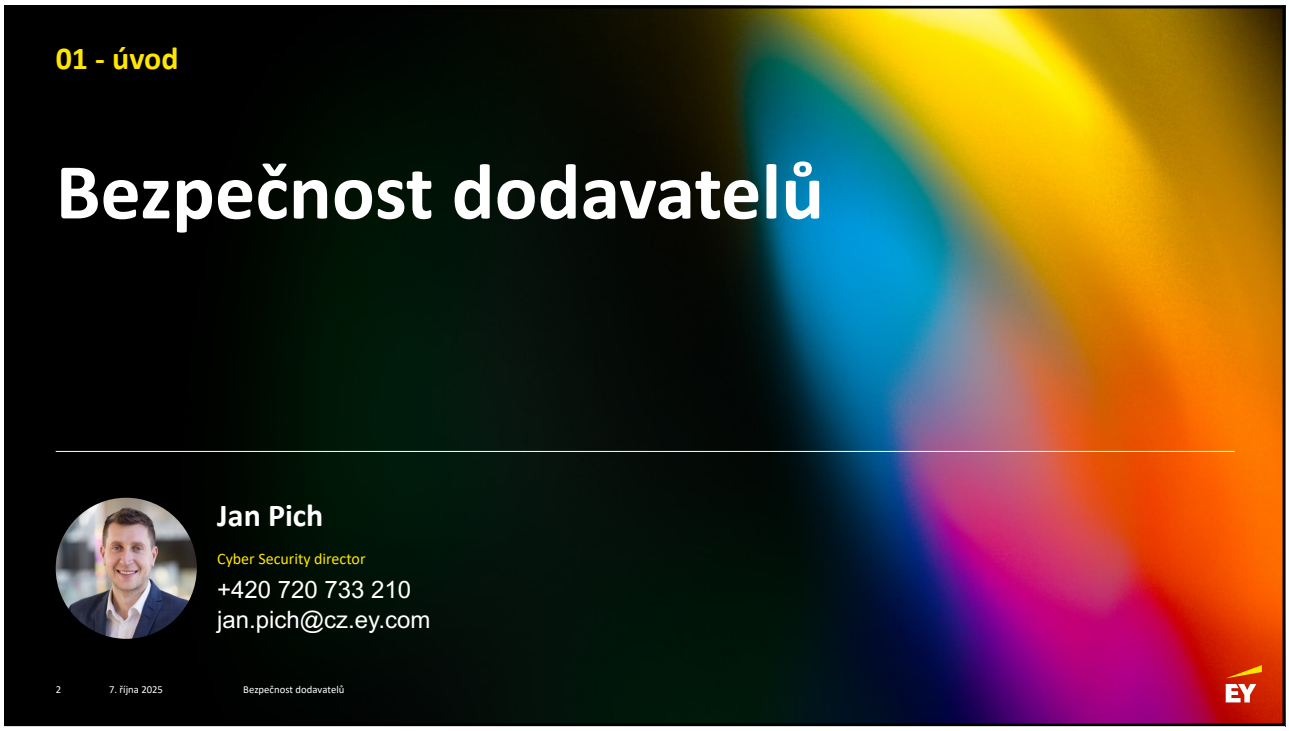

Řízení dodavatelského řetězce
13.10.2025
The better the question. The better the answer. The better the world works.
EY
Shape the future with confidence

1


01 - úvod
Bezpečnost dodavatelů
Jan Pich
Cyber Security director
+420 720 733 210
jan.pich@cz.ey.com
2 7. října 2025 Bezpečnost dodavatelů
EY

2

Rizika dodavatelského řetězce

[1]

#1 Hrozba

2010 | 2020 | **2030** | 2030

- Očekávaný vzrůstající trend četnosti incidentů a škod vlivem dodavatelských řetězců.
- Společnosti jsou lépe chráněny → útočníci útočí prostřednictvím dodavatelů.

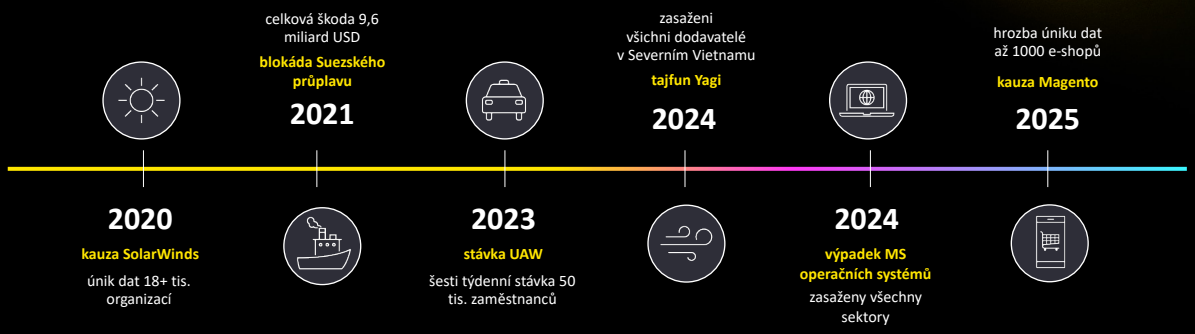
[1] Zdroj: ENISA Foresight Cybersecurity Threats for 2030

3

Útoky přes dodavatele: Nejde o teorii, ale o realitu

4

Některé známé případy výpadků



5

Bezpečnost dodavatelů: Nová pravidla hry

DORA:

"Bezpečnost vašich dodavatelů je vaše odpovědnost." Nestačí jen nakoupit službu, musíte aktivně řídit rizika spojená s celým dodavatelským řetězcem.

vaše **služba** = vaše **odpovědnost**

Každá organizace **nese plnou odpovědnost** za služby, které poskytuje

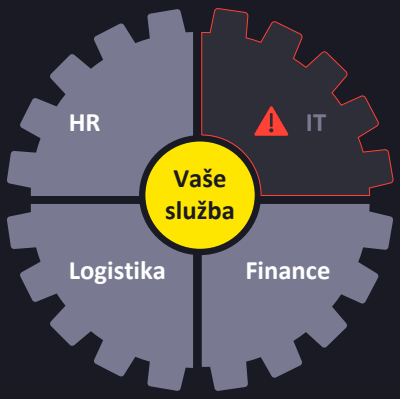
Nezáleží na tom, zda je služba regulována – **zákazníci očekávají spolehlivost**

Proto je nezbytné vědět, že vaši dodavatelé jsou **zabezpečeni a spolehliví**

6

Závislost na dodavatelích

Stačí výpadek jednoho dodavatele
a může dojít k **výpadku celé služby**



- Banky mají desítky ICT dodavatelů a subdodavatelů
- Většina firem **je závislá** na externích dodavatelích
- Výpadek dodavatele → **výpadek celé služby**
- Bezpečnost dodavatelů je dnes **strategická priorita**

7

DORA: Z pohledu ČNB

- **Zvýšená pozornost pojišťovnám**, jelikož ČNB identifikovala vyšší míru rizik než u bank
- Očekávají se **zavedené a funkční procesy**, nikoli pouze projektové plány
- **Registr informací:** povinná evidence všech ICT dodavatelů a jejich subdodavatelů; ČNB bude kontrolovat jeho úplnost a aktuálnost
- **Incident management:** požadavek na rychlé hlášení závažných incidentů a přesné vyčíslení ekonomických dopadů v ročních reportech

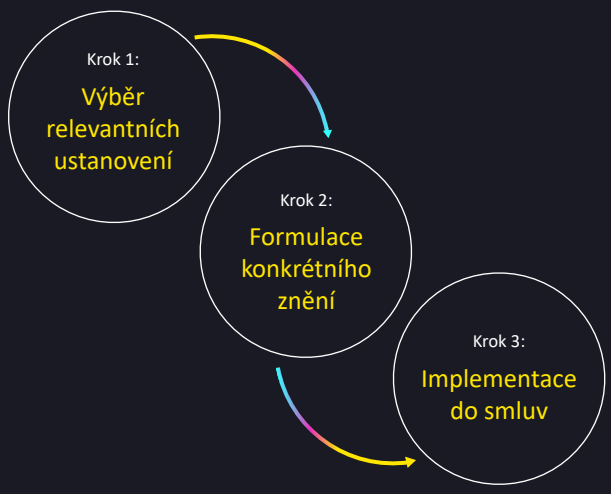
8

Dodavatelé: Proč to je problém?

- Povinnosti podle DORA:
  - Přehled všech dodavatelů **(registr informací)**
  - Smlouvy musí obsahovat **povinné body** (audit, bezpečnost, možnost ukončení)
- Problém: velcí globální dodavatelé často odmítají změny. Regulace ale tlačí na to, aby se přizpůsobili
- ČNB bude chtít vidět, že **řídíte rizika dodavatelů**

9

Smlouvy s dodavateli – právní požadavky



- Povinnost implementovat do dodavatelských smluv relevantní ustanovení, např.:
  - Pravidla řetězení dodavatelů
  - CoC clause
  - Zákaznický audit
  - Exit pravidla
- Dopadá na budoucí, ale i současné smlouvy s dodavateli

10

Kontroly dodavatele

Co musíte aktivně a pravidelně kontrolovat

Evidence a informování:

Musíte vést seznam svých významných dodavatelů
a prokazatelně je informovat o tom, že je jako významné vedete.

11

Je nějaké elegantní řešení?

ANO!

Komplexní due diligence dodavatele.

Automatizované řízení – spolupráce s forenzním týmem EY

Osvědčená podrobná hodnocení a automatizované testy, které poskytují informace o:

- Cybersecurity resilience
- Finanční zdraví
- Rizika subdodavatelů
- Geopolitická a geografická rizika

Veřejně dostupné metodiky

- Belgický CyberFundamentals Framework (link)
- Irské pokyny k zabezpečení dodavatelského řetězce (link)

12

Základní principy DORA pro rizika třetích stran

- DORA povyšuje riziko třetích stran v oblasti ICT z problému IT na primární odpovědnost na úrovni představenstva.
- **rámec pro řízení rizik (článek 6):** DORA vyžaduje komplexní, dobře zdokumentovaný a účinný rámec pro řízení rizik v oblasti ICT.
- Riziko třetích stran nelze řídit izolovaně. Musí být identifikováno, klasifikováno a řízeno se stejnou důsledností jako tradiční finanční rizika, jako je úvěrové riziko nebo tržní riziko.
- **Registr informací (článek 28):** Jsme povinni vést podrobný a průběžně aktualizovaný "Registr informací" o všech smlouvách s poskytovateli služeb ICT třetích stran, a to na úrovni jednotlivého subjektu i konsolidované skupiny. Nejedná se o jednoduchý seznam dodavatelů; musí obsahovat konkrétní údaje o každé službě, o tom, zda podporuje kritickou funkci, a smluvní detaily. Tento registr bude podléhat kontrole ze strany regulátora.

28–31 články

13

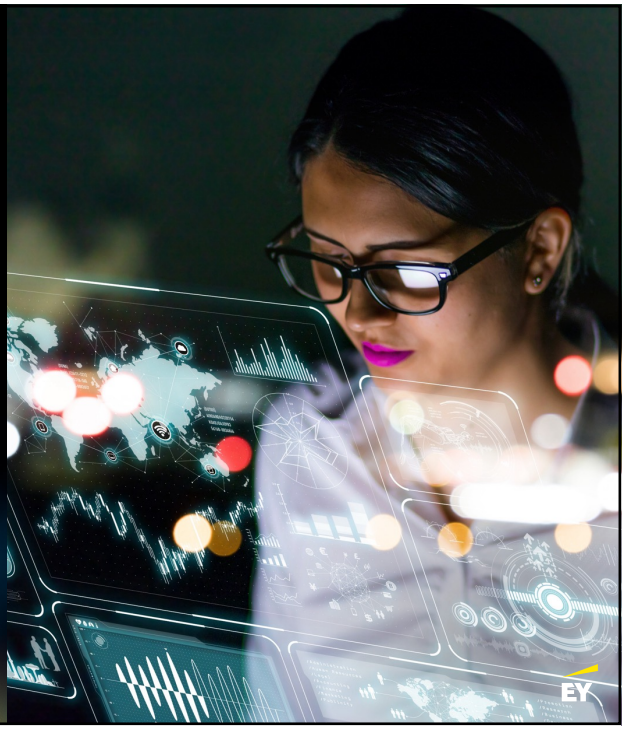
Smluvní mandáty nařízení DORA

- DORA předepisuje specifické, nevyjednávatelné doložky, které musí být zahrnuty ve smlouvách s poskytovateli služeb ICT třetích stran, zejména s těmi, kteří podporují kritické nebo důležité funkce. Naše stávající smluvní šablony musí být přezkoumány a upraveny.
- **Neomezený přístup a práva na audit (článek 30):** Smlouvy musí bance, námi jmenovaným auditorům třetích stran a našim regulátorům udělovat plná práva na inspekci a audit poskytovatele služeb ICT. To zahrnuje přístup ke všem relevantním zařízením, systémům a datovým centrům. "Právo na audit" již nestačí; musí se jednat o neomezené právo.
- **Jasná bezpečnostní ustanovení:** Smlouvy musí specifikovat požadavky na bezpečnost dat, včetně standardů šifrování (pro data při přenosu i v klidu), míst zpracování dat a dodržování našich interních bezpečnostních politik.
- **Hlášení incidentů a spolupráce (článek 29):** Musí být definovány přísné, časově vymezené dohody o úrovni služeb (SLA) pro hlášení bezpečnostních incidentů bance. Dodavatel se musí zavázat k plné spolupráci během reakce na incident, vyšetřování a nápravných opatření.
- **Účast na bezpečnostním testování (článek 26):** Kritičtí dodavatelé služeb ICT musí být smluvně zavázáni k účasti v našich pokročilých programech bezpečnostního testování, jako je penetrační testování na základě hrozeb (TLPT). Tím je zajištěno, že můžeme testovat naši odolnost napříč celým řetězcem poskytování služeb.

14

Soulad s DORA není jednorázové posouzení; je to nepřetržitý životní cyklus dohledu.

- **Nepřetržité monitorování**
- **Posouzení rizika koncentrace (článek 28)**
- **Povinné, testovaní strategie ukončení (článek 28)**



15

Exit strategie / Plán Regulatorní požadavky

Podle očekávání PRA SS2/21 je nutné při plánování ukončení všech významných smluvních vztahů zohlednit tyto klíčové požadavky:

Hlavní principy	Co to znamená v praxi
Všechny významné smlouvy s třetími stranami musí mít zdokumentovanou exit strategii	Soulad s rámcem pro ukončení třetích stran, s minimálními odchylkami
Exit strategie musí zajistit kontinuitu klíčových funkcí při plánovaném i neplánovaném ukončení	Proces zajišťující správné zachycení dat a snížení rizik v rámci exit procesu
Exit strategie musí obsahovat postupy pro zmírnění rizik jako poslední možnost při vážném narušení provozu	Proces umožňující pochopení rizik spojených s významnými smlouvami
Exit strategie musí být pravidelně testována, např. každoročně	Podpora při budování odolnosti a schopností obnovy klíčových funkcí
	Proces pro dokončení ukončení smluvního vztahu
	Zajištění odpovědnosti za přezkum plánů dle regulatorních požadavků
	Zajištění odpovědnosti za přezkum plánů správnými zdroji pro omezení rizik

16

Exit strategie / Plán

Příklad exit strategie

Interní dokumenty	1. Informace o smlouvě 2. Detaily subdodavatelů 3. Role a odpovědnosti 4. Hodnocení dopadu na podnikání 5. Řízení exit strategie 1. Hodnocení rizik 2. Lhůty oznámení ukončení 3. Časový rámec přechodu 4. Komunikační plán	Agregují se všechny relevantní informace o třetí straně nebo skupinové smlouvě, stejně jako o smluvních službách, které jsou důležité při tvorbě exit strategie a exit plánu
	6. Definice exit strategie 1. Plánované ukončení 2. Neplanované ukončení	Detailně se popisují aktivity a specifikují se požadavky, aby bylo zajištěno splnění cílů exit strategie
Dokončeno s třetí stranou	7. Exit plán	Popisuje zapojení třetí strany nebo skupiny před, během a po ukončení
	8. Testování exit strategie	Poskytuje rámec a pokyny pro testování exit strategie a plánu

17

Co odnést na závěr

Obecné požadavky na řízení rizik třetích stran

Níže je uveden přehled klíčových požadavků, které je třeba vzít v úvahu při vývoji strategie řízení rizik třetích stran.

Definice a rozsah	Před outsourcingem	Sub-outsourcing
▪ Stanovit **provozní model** ▪ Přizpůsobit procesy (využití skupinových postupů)	▪ Definovat **nástroje pro hodnocení rizik /** kritéria ▪ Proces oznámení regulátorovi (např. šablona)	▪ Posílit **rámec pro sub-outsourcing** ▪ Mít jasné dohody
Proporcionalita	**Smluvní dohody**	**Přístup a audit**
▪ Aktualizovat / rozšířit **rámec pro dohled** (včetně monitorovacích procesů) ▪ Nastavit eskalační procesy (spolu s odpovídajícími SLA / KPI / KRI)	▪ Aktualizovat rámec pro procesy uzavírání smluv ▪ Zahrnout aspekty odolnosti; mapování pro jednotlivé jurisdikce ▪ Aktualizace smluv	▪ Úpravy katalogu poskytovaných služeb, zajištění a požadavky na reporting rizik ▪ Požadavky na registr outsourcingu
Governance	**Bezpečnost dat**	**Kontinuita podnikání / Exit strategie**
▪ Vypracovat požadavky na reporting ▪ Propojit s operační odolností (zajistit zohlednění prahových podmínek) ▪ Zavést RACI matice (Role, Odpovědnosti, Konzultace, Informace)	▪ Aktualizovat rámec pro řízení rizik a kontrol (dle místních regulatorních požadavků – kde je to nutné) ▪ Provést přezkum v souladu se skupinovým rámcem pro data	▪ Aktualizovat skupinové šablony a procesy pro BCP / Exit ▪ Zohlednit toleranci dopadu a testování scénářů v dokumentaci

18

Shrnutí a klíčové myšlenky

Kyberbezpečnost je strategické téma s přímou odpovědností vedení.

- Nový zákon ji povyšuje na úroveň financí nebo práva. Nejde jen o "IT problém".
- Hrozí zde **osobní odpovědnost** (náhrada škody, zákaz činnosti).

Řízení rizik je základ všeho.

- Zákon nevyžaduje plnění checklistu, ale **přemýšlení o reálných hrozbách** a přijímání přiměřených opatření.
- Klíčové je porozumět, co je pro vaši firmu kritické, a chránit to.

Vaše bezpečnost končí tam, kde začíná bezpečnost vašeho dodavatele.

- Dodavatelé jsou častým cílem útoků a vy za ně nesete odpovědnost.
- **Prověřujte, smluvně ošetřete a pravidelně kontrolujte** své partnery.

Harmonogram je neúprosný.

- **Účinnost zákona:** 1. listopadu 2025
- **Registrace u NÚKIB:** do 31. prosince 2025
- **Zavedení všech opatření:** do roka od doručení oznámení z NÚKIB

19

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

20