

GDPR po roku:

Praktické skúsenosti s prihliadnutím na pozíciu zodpovednej osoby

Jindřich Kalíšek, Ph.D. CIPP/E CIPM

Advokát a zodpovedná osoba pre spoločnosti skupiny KKCG

Přednášející

Jindřich Kalíšek

Advokát se specializací na IP/IT, cyber/infosec a ochranu osobních údajů

- Člen Sekce České advokátní komory pro právo IT a GDPR
- 25 implementačních projektů v letech 2017-2018

Pověřen pro vybrané společnosti privátní investiční skupiny KKCG

- Sazka a.s. (největší česká sázková a loterijní společnost / alternativní mobilní operátor)
- Cestovní kancelář FISCHER, a.s.
- MND a.s. (dodavatel energií a služeb)
- DataSpring s.r.o. (poskytovatel hostingu / cloudových služeb)
- Conectart s.r.o. (telemarketér a provozovatel zákaznických linek)



Témata příspěvku

- GDPR Update 2019
- Jaký je správný přístup k GDPR compliance a jaké jsou pravidelné rizikové scénáře a situace?
- Nakládání s osobními údaji (OÚ) je povinnou náležitostí podnikatelské strategie
- GDPR je norma nepřehledná a kontradiktorní (a díkybohu za to)
- Desatero (minimální) GDPR compliance
- „Nice-to-have“ nástroje k dosahování GDPR compliance
- Kde najít vhodná TOMs?
- GDPR a to okolo – vztahy s kybernetickou a informační bezpečností
- Proč to všechno vlastně řešit?

GDPR Update I

GDPR v roce dva (2019)

- Adresáti „plavou“ v základních principech a požadavcích GDPR
- Roste sebevědomí DPA a subjektů údajů
 - 65 000 hlášení data breaches a 200 000 stížností subjektů OÚ vůči DPA
- Konec doby hájení ze strany úřadů (ICO v UK, Irsku, CNIL, dánský úřad) a *documentation-only* přístupu
- První soudní spory a „drakonické“ sankce
- Chybějící samoregulace (kodexy chování, BCR)?

Výhled

- Sladění ochrany osobních údajů s ochranou neosobních informací a kyberbezpečnostními standardy
- GDPR je kamínek, který odstartoval lavinu technologické regulace
 - USA (Kalifornie, NY), Asie (AIPAC „GDPR“) a Austrálie
 - Nařízení o volném toku neosobních údajů
 - Kyberbezpečnostní nařízení EU
 - Novely oborové regulace, které inkorporují technická opatření



GDPR Update II

Úniky osobních údajů

- Mediálně vděčné případy úniků osobních údajů →
 - Obrovská reputační rizika a kolaterální škody
 - Koncerny a podnikatelská uskupení – non-compliance malé části skupiny může mít zásadní dopady na celou skupinu

Aadhaar (1,1 mld. záznamů)	MyHeritage (92 mil. záznamů)
Marriot (500 mil. osob)	Facebook (87 mil. záznamů → reálný dopad řádově vyšší)
Under Armour → MyFitnessPal (150 mil. záznamů)	Ticketfly (27 mil. záznamů)

Sankce v EU (2018)

11 států a celkem 63 milionů € → Přeshraniční vyšetřování a ukládání pokut?

50 milionů € – Francie (Google)	80 tisíc € – Německo, Baden-Württemberg
400 tisíc € – Portugalsko (dvě nemocnice)	50 tisíc € – Itálie
220 tisíc € – Polsko (Biznode)	35 tisíc € – Maďarsko (politická strana DK)
170 tisíc € – Norsko (město Bergen)	20 tisíc € – Německo (Knuddels.de)
160 tisíc € – Dánsko (taxi společnost)	5 tisíc € – Malta (Lands Authority)

Sankce v ČR

- § 63 z. č. 110/2019 Sb. → max. 10 mil. Kč (≈ 390 tisíc €) → zcela vyloučeny veřejné subjekty

Správný přístup × Rizikové scénáře ?

Správný přístup

- Přinejmenším minimální GDPR compliance v rozsahu 7+3
- Rozumná aplikace požadavků s přihlédnutím k prostředí, potřebám a možnostem organizace a jejímu rizikovému profilu (!)
- Integrace do všech procesů a evidencí organizace (i kdyby postupná)
 - Zásady ochrany a zabezpečení osobních údajů (čl. 25 + 32 GDPR)
 - DPIA
 - Change management / Procurement
- Řízené pravidelné zlepšování
 - *Tone from the top*
 - Vzdělávání a zvyšování risk-awareness



Typické rizikové scénáře

Potěmkinova vesnice

Dělo na vrabce

Spekulativní ignorace / Rezignace

Typické aplikační problémy

Chybějící reflexe principů ochrany a zabezpečení osobních údajů

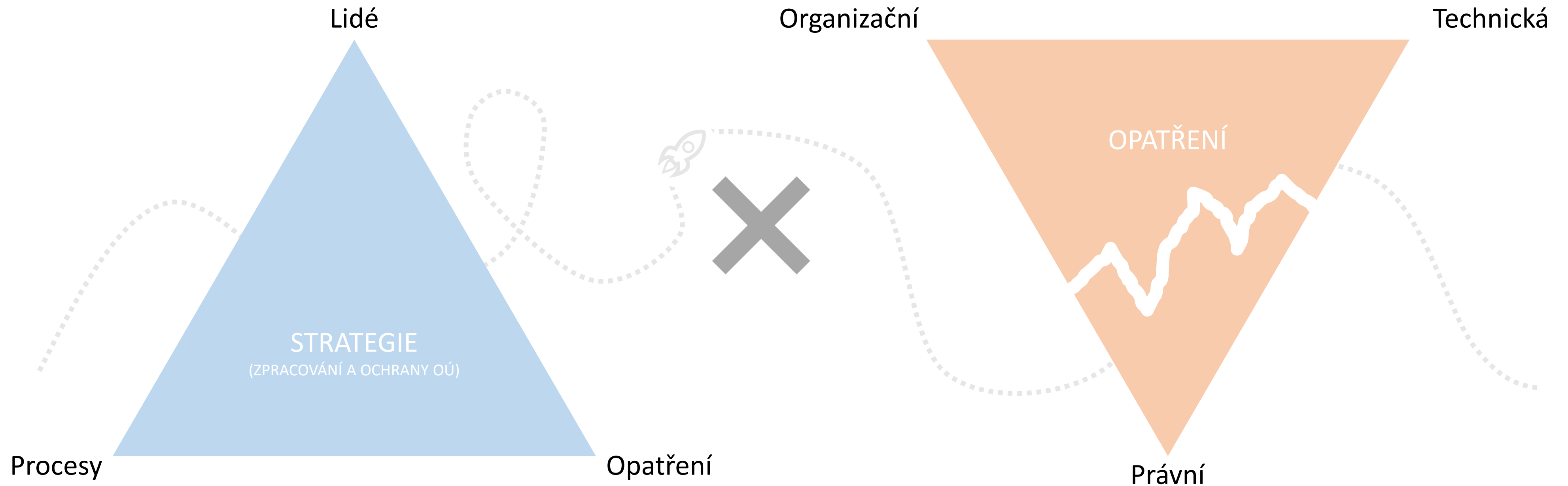
Nedostatečná dokumentace shody

Nedostatečná příprava a implementace prostředí, procesů a opatření

Smlouvy o zpracování osobních údajů a další smluvní vztahy související s nakládáním s informacemi



Nakládání s OÚ je (povinná) součást Vaší strategie



Zásady zpracování a ochrany OÚ jsou vzájemně kontradiktorní

Základní principy GDPR

- Zásada odpovědnosti (čl. 74 recitálu + čl. 5 odst. 2 GDPR)
 - Povinnost správce dodržet všechny povinnosti vyplývající ze zásad
 - Povinnost správce dodržení shody prokázat
- Přístup založený na vyhodnocení rizik (čl. 75-78 recitálu + čl. 25 a 32 a násl. GDPR)
- Účely zpracování (čl. 39 recitálu + čl. 6 GDPR)

Zásady zpracování OÚ (čl. 39 recitálu + čl. 5 odst. 1 GDPR)

- Zásada zákonnosti, korektnosti a transparentnosti zpracování
- Zásada účelového omezení shromažďování osobních údajů
- Zásada minimalizace zpracovávání osobních údajů
- Zásada přesnosti osobních údajů
- Zásada omezeného uložení OÚ
- Zásada integrity a důvěrnosti zpracování

Zásady ochrany OÚ (čl. 78 recitálu + čl. 25 GDPR)

- Zásada záměrné ochrany OÚ (*Privacy by Design*)
- Zásada standardní ochrany OÚ (*Privacy by Default*)

Zabezpečení OÚ (čl. 78 recitálu + čl. 32 GDPR)

- Správce a zpracovatel jsou povinni zavést vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení OÚ odpovídající danému riziku
- Správce a zpracovatel při posuzování požadované úrovně bezpečnosti a výběru a implementaci opatření zohlední *stav techniky, náklady na provedení, povahu, rozsah, kontext a účel zpracování, rizika pro práva a svobody fyzických osob*

Desatero (minimální) GDPR compliance

Soubor požadavků, které jsou mandatorní pro každého správce, potažmo zpracovatele

- Součástí minimální přípravy musí být od počátku vyhodnocení rizik a zohlednění rozsahu, obsahu a kontextu zpracovávaných OÚ
 - Aktuální dokumentace naplňování zásad zpracování a ochrany OÚ dle čl. 5, 6, 25 a 32 GDPR → **vyhodnocení významných a koncepčních rizik včetně IT, definice role IT**
 - Aktuální záznamy o zpracování OÚ dle čl. 30 GDPR → **úvodní hodnocení rizik, pravidelná aktualizace**
 - Naplňování informační povinnosti vůči subjektům údajů dle čl. 12 – 14 GDPR
 - Proces naplňování práv subjektů údajů dle čl. 15 – 24 GDPR a vedení jejich evidence → **předcházení bezpečnostním incidentům včetně IT**
 - Proces identifikace, vyhodnocení a hlášení bezpečnostních incidentů a vedení jejich evidence → **podrobná analýza rizik – imanentní součást činností IT**
 - Revize a renegociace smluv → smlouvy o zpracování OÚ dle čl. 28 GDPR → řízení rizik v dodavatelském downstreamu
 - Systém evidence souhlasů subjektů se zpracováním OÚ
- Pravidelné zlepšování, zajišťování awareness a testování prostředí
 - Ustavení a zajištění funkce DPO → **přístup, zapojení do řízení, pravidelný risk assessment**
 - Provedení posouzení vlivů na zpracování OÚ (DPIA) → **podrobné hodnocení rizik**

„Nice-to-have“ nástroje



GDPR Compliance Repository

- Nástroj pro prokazování compliance
 - Zásada odpovědnosti
 - Zásada přístupu založeného na řízení rizika

Obsah

- Souhrnná auditní / analytická zpráva
- Záznamy o činnostech zpracování
- Balanční testy
- Vnitřní normy a řídicí dokumentace
- Dokumentace informační povinnosti vůči subjektům údajů
- Dokumentace práv subjektů údajů
- Smlouvy o zpracování OÚ
- Procesy identifikace a hlášení bezpečnostních incidentů
- Záznamy o DPIA

Forma

- Elektronická dokumentace (uložiště) × Fyzický otisk (šanon)



GDPR Compliance (Self-)Assessment

- Interní metodika pro hodnocení GDPR compliance
- Hodnocení, testování, udržování a průběžné zlepšování compliance společností
- Hodnocení a testování compliance u obchodních partnerů společností KKCG
- 15+ metrik
- Základní metriky + Vedlejší metriky = Hodnotící agregát (v %) → Každá metrika má hodnotící kritéria, úkoly a kontrolní body
 - Popis procesů a procesní governance
 - Záznamy o činnostech zpracování a evidence
 - Správa a řízení práv subjektů
 - Smlouvy s třetími stranami a datové přenosy
 - Datová bezpečnost a *Data Breach Management*
 - Komunikace, školení, vzdělávání
 - Audit

Kde najít vhodná TOMs?

GDPR neobsahuje žádný srozumitelný katalog TOMs

Pracuje s notoriemi *vhodná technická a organizační opatření* (TOMs) × *bezpečnostní opatření*, ale nedefinuje je

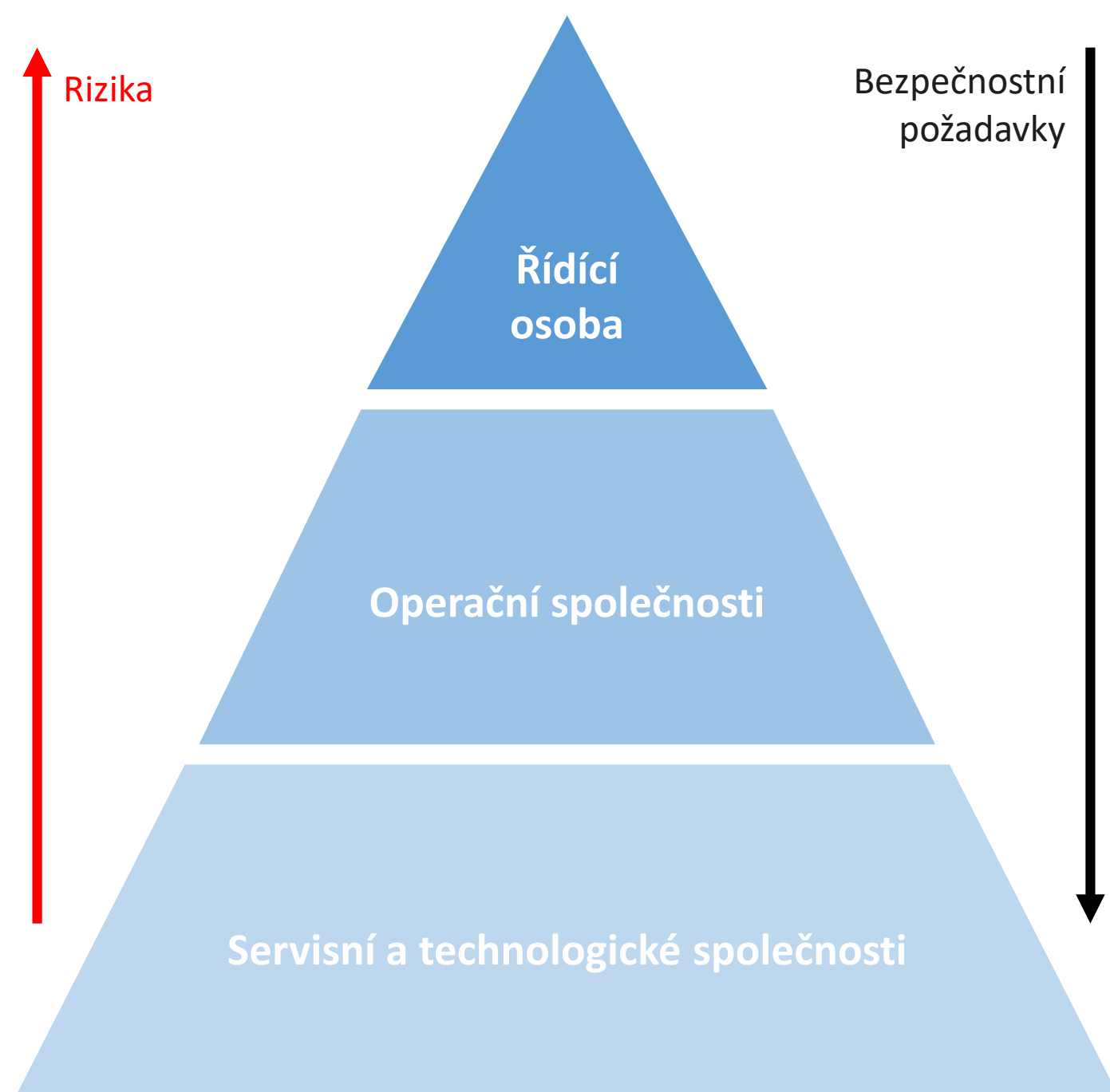
Katalogy vhodných bezpečnostních opatření

- Mezinárodní úmluvy a evropské normy (nařízení, směrnice)
- Zákon o kybernetické bezpečnosti a jeho prováděcí právní předpisy
- Zvláštní zákony pro jednotlivé, specificky rizikové oblasti (bankovníctví, pojišťovnictví, zdravotnictví, energetika, doprava) → často nekomplexní anebo právně nevymahatelné úpravy
- Podzákonná regulace odbornými orgány veřejné moci
- Oborová regulace vytvářená ústředními správními úřady a dozorovými orgány
 - NÚKIB / NBÚ / MV ČR, ČNB, ERÚ, SÚKL
 - (úřední sdělení – cloud computing, operační rizika v S/IS apod.)

Oborové technické normy a standardy

- ISO IEC 27 001 a násl.
- ISO IEC 29 134

Ochrana OÚ, CS/IS a to okolo



Pyramidová konstrukce bezpečnosti

- Strategické požadavky na bezpečnost směrem vzhůru rostou ×
- Schopnost exekvovat bezpečnostní politiky směrem vzhůru klesá
- Technické a organizační přístupy musí koncipovat organizace v základu pyramidy, které ji poskytují ostatním jako službu
- *Cyber Security as a Service* (CSaaS)

Spojené nádoby informační / kybernetické bezpečnosti a ochrany OÚ

- Bezpečnostní incident ≈ Incident na poli ochrany OÚ ≈ Incident na poli ochrany obchodních tajemství a důvěrných informací
 - Neoprávněné zpřístupnění OÚ / obchodních informací
 - Zničení / ztráta OÚ / obchodních informací
 - Ztráta telefonu / hardware
 - Kompromitace identity / credentials odposlechnutím hesel
- Dopady bezpečnostního incidentu nemusí být hned zřejmé
 - Nutná analýza možných dopadů do sféry OÚ/obchodních informací
 - Možná povinnost hlásit ÚOOÚ a dalším regulátorům
 - Druhotné dopady závažnější než přímé ztráty

Dopady GDPR do obecné CS/IS

GDPR vyžaduje robustní a systematicky budovanou infrastrukturu kybernetické a obecné informační bezpečnosti

- GDPR pravidelnou součástí regulatory & compliance DD
- Reputační riziko ← únik OÚ znamená zpravidla nedostatky i v dalších oblastech

Vhodná organizační opatření

- Compliance Repository
- Řízení subdodavatelských řetězců a třetích stran (audity, certifikace)
- Pravidelné školení a vzdělávání
- Řízení politik a procesů
- Geografická relokační citlivých údajů

Vhodná technologická opatření

- Identity & Access Management (IDAM)
- Data Loss Prevention (DLP)
- Šifrování a anonymizace (Encryption & Pseudonymization)
- Master Data Management / Data classification

Proč tomu všemu věnovat pozornost?



Protože stačí jeden (nepříliš agilní) útočník s (vcelku primitivní) technologií...

- Útoky a ztráty jsou častější, složitější a zvyšuje se jejich rizikovost → Rostou přímé náklady na sanaci škod a sankce
- Data jsou dnes nejhodnotnějším aktivem × náklady na útok jsou marginální

Kolaterální škody

- Blacklisting / Ztráta ratingu / ztráta obchodních příležitostí
- Snížení hodnoty podniku / koncernu (efekt nákazy)
- Globální reputační riziko
- Postih v související oblasti → kompromitace v jedné oblasti odhaluje rizika jinde

Nezbytná součást byznysu

- Externí dopady – data protection check se stává pravidelnou součástí investičních DD → řízení rizikovosti transakcí, předcházení adjustacím kupních cen
- Interní dopady ← Dlouhá doba prevalence rizik
- KYC → KYT²



Ďakujem za pozornosť

Jindřich Kalíšek

@: jindrich.kalisek@kkcg.com
jindrich@kalisek.net

W: www.kkcg.com

Jindřich Kalíšek, Ph.D. CIPP/E CIPM

Advokát a zodpovedná osoba pre spoločnosti skupiny KKCG