LGP
LANSKY, GANZGER, JACKO + PARTNER
RECHTSANWÄLTE / ATTORNEYS

MOORE BDR

DXC TECHNOLOGY

AON

Business raňajky:
Kybernetická bezpečnosť vo firmách
23. apríla 2025

SLOVENSKO - RAKÚSKA OBCHODNÁ KOMORA
SLOWAKISCH - ÖSTERREICHISCHE HANDELSKAMMER

SWEDISH CHAMBER OF COMMERCE IN SLOVAKIA

CAMERA DI COMMERCIO ITALO - SLOVACCA
CAMERE DI COMMERCIO ITALIANE ALL'ESTERO

+ LGP

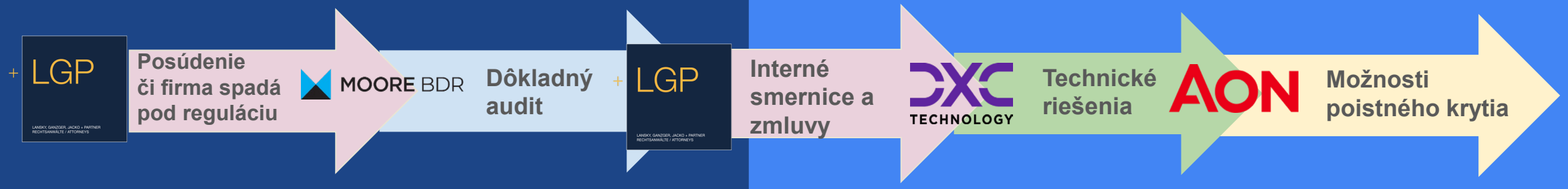
LANSKY, GANZGER, JACKO + PARTNER
RECHTSANWÄLTE / ATTORNEYS

SLOVENSKO - RAKÚSKA OBCHODNÁ KOMORA
SLOWAKISCH - ÖSTERREICHISCHE HANDELSKAMMER

SWEDISH CHAMBER OF COMMERCE IN SLOVAKIA

CAMERA DI COMMERCIO ITALO - SLOVACCA
CAMERE DI COMMERCIO ITALIANE ALL'ESTERO

Kybernetická bezpečnosť
Implementácia v obchodnej spoločnosti



LGP

Dopadová analýza zákona o kybernetickej bezpečnosti

Ciele:
Identifikácia subjektov spadajúcich pod definíciu prevádzkovateľa základnej služby.

Praktické kroky:
Konzultácie, analýza procesov, právne posúdenie, návrh odporúčaní.

Výstup:
Dokument – dopadová analýza a jej prezentácia výsledkov

LGP

Registrácia do zoznamu

- Registrácia do zoznamu prevádzkovateľov základných služieb do 60 dní od začiatku činnosti.
- Podanie návrhu na zápis prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

MOORE BDR

SLOVENSKO - RAKÚSKA OBCHODNÁ KOMORA
SLOWAKISCH - ÖSTERREICHISCHE HANDELSKAMMER

SWEDISH CHAMBER OF COMMERCE IN SLOVAKIA

CAMERA DI COMMERCIO ITALO - SLOVACCA
CAMERE DI COMMERCIO ITALIANE ALL'ESTERO

MOORE TECHNOLOGY

NIS2 a zákon 366/2024

MOORE

HELPING YOU THRIVE IN A CHANGING WORLD

OPATŘENÍ SPOJENÁ S NIS2

První kroky pro povinné organizace

Zákon č. 366/2024 Z. z., účinný od 1. januára 2025, novelizuje zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti.

Jeho hlavným cieľom je transpozícia smernice NIS 2 (smernica (EÚ) 2022/2555) do slovenského právneho poriadku, čím sa zvyšuje úroveň kybernetickej bezpečnosti na národnej úrovni a reaguje sa na výzvy spojené s digitalizáciou a technologickým vývojom.

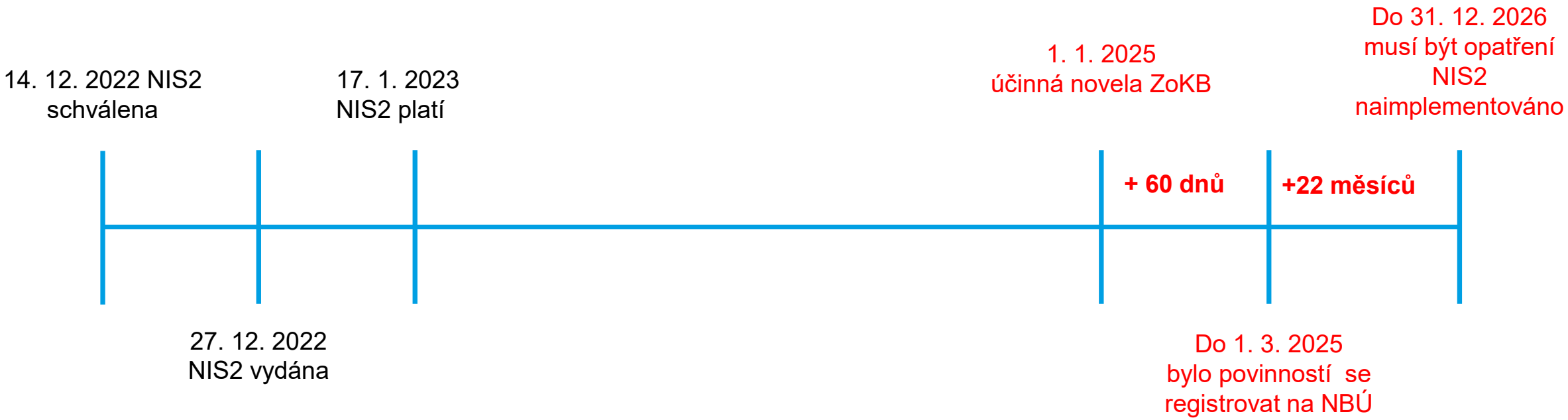
Prvním krokem pro povinné subjekty je ohlášení na NBÚ! ….. které mělo proběhnout *do 1.3.2025*

SMĚRNICE NIS2 – časová osa SVK

NIS2 – směrnice EU o kybernetické bezpečnosti s platností od 17. 1. 2023

Dne 14. prosince 2022 přijala Evropská komise **Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti (NIS2) v celé Unii.**

Nyní tuto směrnici zapracovává **NBÚ Slovensko** do nového znění **zákona o kybernetické bezpečnosti**.
Návrh směrnice zároveň požaduje, aby členské státy sestavily seznam povinných subjektů.



OPATŘENÍ SPOJENÁ S NIS2

První kroky pro povinné organizace

- **Dopadová analýza** o určení povinnosti k zákonu o KB a ohlašovací povinnost
- **Rozdílová analýza** pro určení aktuálního stavu KB v organizaci
- **Implementace:**
- Zavedení bezpečnostní politiky, identifikace aktiv a analýza rizik
- Tvorba dokumentace a důkazních materiálů
  (Záznamy o incidentech, BCP/DR, záznamy o školení)
- Jmenování odpovědných osob
- Implementace technických a organizačních opatření dle bezpečnostní politiky
- Školení zaměstnanců v KB
- Vyžadování KB standardů od klíčových dodavatelů
- **Udržování a rozvoj opatření ochrany KB:**
- Audit – ověření implementace – nápravná opatření
- Neustálý rozvoj a zlepšování KB v organizaci, revize bezpečnostní politiky na základě výsledků auditu a rozvoje organizace

DXC TECHNOLOGY

SLOVENSKO - RAKÚSKA OBCHODNÁ KOMORA
SLOWAKISCH - ÖSTERREICHISCHE HANDELSKAMMER

SWEDISH CHAMBER OF COMMERCE IN SLOVAKIA

CAMERA DI COMMERCIO ITALO - SLOVACCA
CAMERE DI COMMERCIO ITALIANE ALL'ESTERO

Technologické opatrenia vyplývajúce z 366/2024 Z.z.

Technické opatrenia v oblasti kybernetickej bezpečnosti

- **Vychádzajú zo schválenej bezpečnostnej dokumentácie organizácie**
  - Bezpečnostnej stratégie
  - Bezpečnostnej politiky

- **GAP analýza**
  - evidencia aktív / dáta, IS, nástrojov KB
  - zistené nedostatky
  - návrh na odstránenie

- **ToBe stav**
  - návrh doplnenie ochrany
  - re-design systémov
  - výmena za nový

Oblasti IT analýzy

- súvisiacej infraštruktúry výrobných a produkčných technológií
    - je prostredie izolované / bez prístupou na internet
    - možnosť upgradu, garancia vendorom

- súvisiacej infraštruktúry informačno-komunikačných technológií
    - backoffice procesy,
    - komunikačné nástroje,
    - CRM, ...

- súvisiacej aplikačnej architektúry,
    - dátova a aplikačná architektúra
    - správa oprávanení
    - komunikačná architektúra / intra vs inter
    - podpora investigatívy / foreznych postupov

- súvisiacej bezpečnostnej architektúry a implementovaných bezpečnostných opatrení,
    - sieťová komunikácia
    - riadenie prístupov
    - centralizácia logov / SIEM
    - manažment zraniteľnosti

Návrh zmien

- **Doplnenie technológii**
  - klasické, cloudové, AI nenabled
- **Trasformácia systémov**
  - Morálne zastaranie
  - Segmentové požiadavky
- **Využívanie platformových služieb**
  - Manažment zraniteľností
  - SIEM, SECaaS a pod.

Revízia dokumentov a procesov

Zabezpečenie súladu so zákonom:

- Asistencia pri príprave a revízií bezpečnostnej dokumentácie.
- Príprava smerníc a interných predpisov.

Revízia zmlúv a interných smerníc:

- Zodpovednosť manažmentu a zamestnancov.
- Zmluvy s externými dodávateľmi IT.

Postup po vzniku incidentu:

- Nastavenie úloh zamestnancov, školenia.

LGP

Riadenie kybernetických incidentov

Postup oznamovania incidentov:

- Včasné varovanie – do 24 hod,
- Oznámenie o incidente – do 72 hod,
- Závrečná správa – najneskôr 1 mesiac.

Koordinácia riešenia incidentov:

Spolupráca s CSIRT, NBÚ,
Úradom na ochranu osobných údajov

Pokuty:

PKZS – 10 mil. EUR / 2% obrat
PZS – 7 mil. EUR/ 1,4 % obrat

LGP

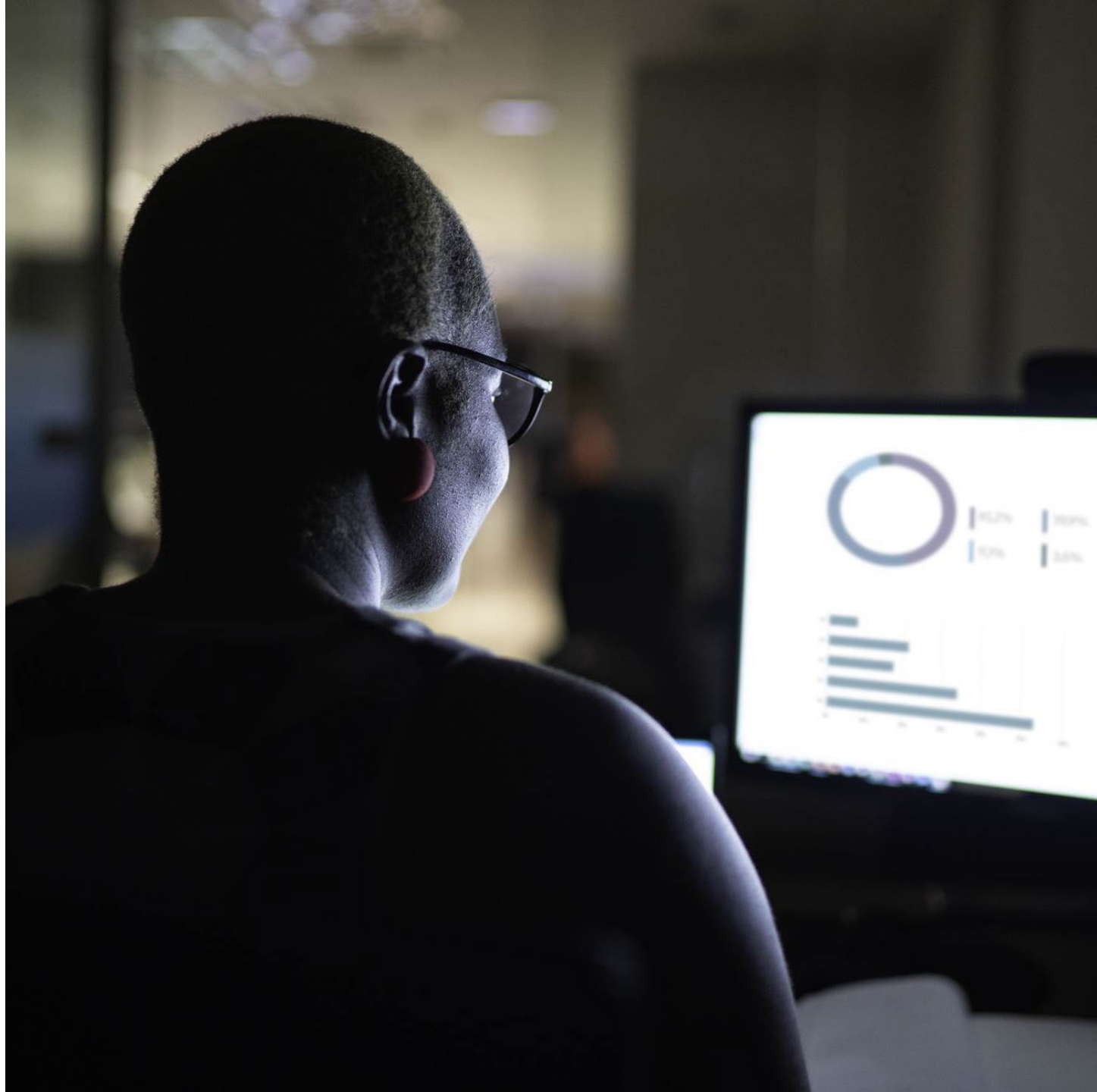
AON

SLOVENSKO - RAKÚSKA OBCHODNÁ KOMORA
SLOWAKISCH - ÖSTERREICHISCHE HANDELSKAMMER

SWEDISH CHAMBER OF COMMERCE IN SLOVAKIA

CAMERA DI COMMERCIO ITALO - SLOVACCA
CAMERE DI COMMERCIO ITALIANE ALL'ESTERO

Rola poistenia pri zvládaní kybernetických incidentov



Hlavné piliere krytia kybernetických rizík

1 Reakcia na incidenty a asistenčné služby

- Krízový manažér
- Právne poradenstvo
- IT forenzné služby
- Náklady na oznámenie
- Náklady na vzťahy s verejnosťou (PR)

2 Krytie vlastných rizík

- Ransomware (vydieranie)
- Prerušenie prevádzky a dodatočné náklady
- Závislé prerušenie prevádzky
- Náklady na obnovu dát
- Náklady na obnovu HW/SW
- Cyber crime (sublimit)

3 Krytie rizík voči tretím stranám

- Narušenie súkromia alebo bezpečnosti siete
- Porušenie ochrany údajov
- Pokuty uložené Dozorným orgánom
- Štandardy pre zabezpečenie údajov o platobných kartách (PCI-DSS)
- Náklady na právnu ochranu

Dodatočné služby s pridanou hodnotou

Cyber poistenie často dopĺňajú služby, ktoré ponúka buď poisťovateľ alebo maklér.
Tieto služby sú individuálne, ale môžu zahŕňať:

- Phishingové a penetračné testy
- Simulovanie incidentov
- Vonkajšie skenovanie siete, aplikácií na identifikovanie rizikových miest
- Prístup k vopred preverenným poskytovateľom odborných služieb
- Informácia o stave kybernetickej odolnosti (zahrnutá pri posudzovaní možnosti poistenia spoločnosti na trhu)

AON

GAP analýza Cyber poistenia

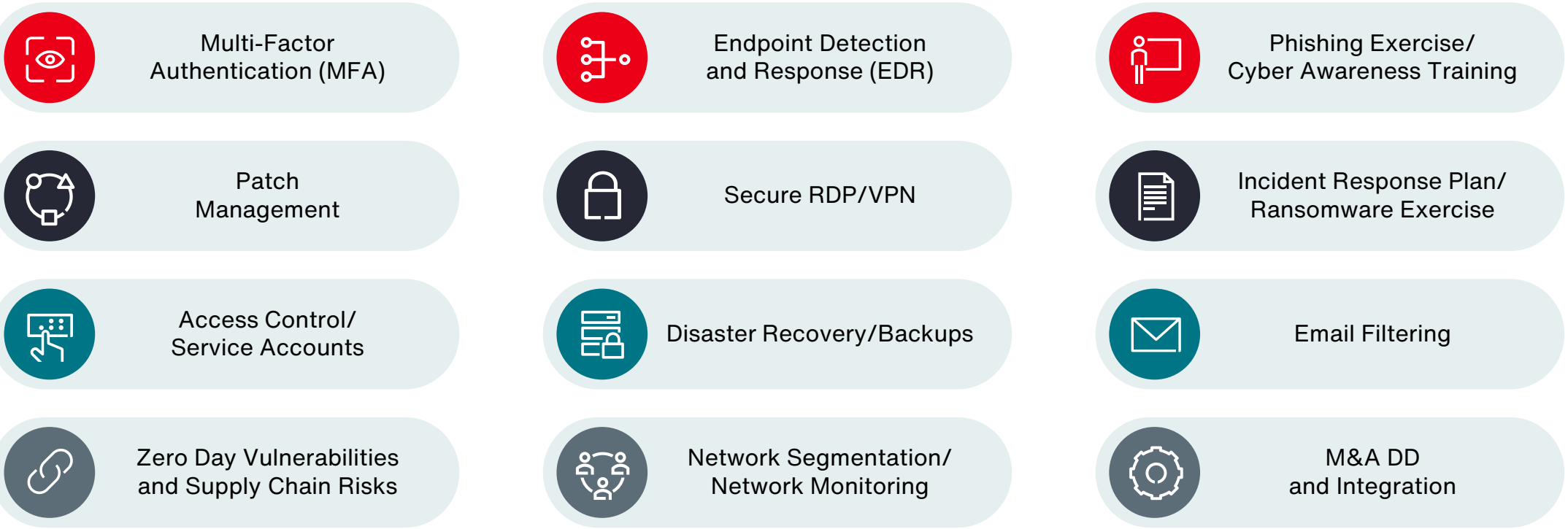
Riziko	Cyber	Profesijná zodpovednosť pri poskytovaní IT služieb	Poistenie Majetku	Poistenie sprenevery (Crime)	Všeobecná zodpovednosť
Prerušenie prevádzky spôsobené kybernetickým incidentom					
Náklady na reakciu na incident po kybernetickom incidente				Potenciálne pokrytie niektorých nákladov	
Peňažná strata spôsobená narušením bezpečnosti alebo kompromitáciou e-mailu (Cyber-Crime)	Iba pre menšie riziká a na sublimit				
Ransomware (vydieranie)				Potenciálne pokrytie niektorých nákladov	
Ohováranie, urážka na cti, hanobenie	(online)	Potenciálne zahrnuté ako súčasť odborných služieb			
Zlyhania technológie vedúce k finančným stratám	Vylúčené ako súčasť odborných služieb, obmedzené na bezpečnostné poruchy				
Fyzické škody spôsobené kybernetickým incidentom	Cyber zahŕňa iba prvok „Bricking“	Potenciálne zahrnuté ako súčasť odborných služieb	Vylúčené alebo „silent“		Potenciálne krytie ako súčasť produktu poskytovanej služby
Zodpovednosť za porušenie ochrany súkromia a bezpečnosti		Potenciálne zahrnuté ako súčasť odborných služieb			Vylúčené alebo „silent“

AON

Red Flags

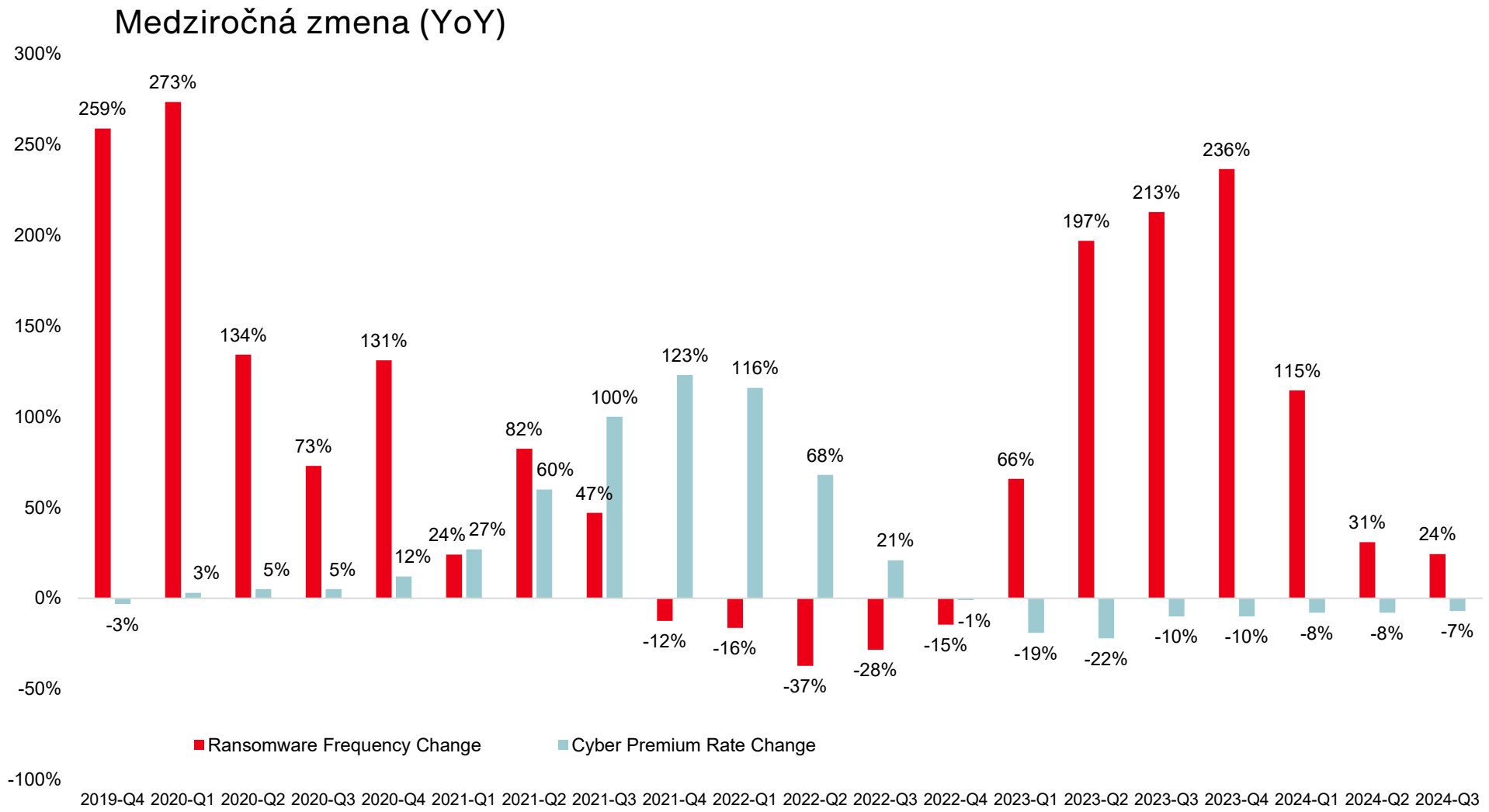
Vyhodnocovanie podkladov z hľadiska ‘red flags’ pri úpise rizika

- Poisťovatelia sa detailne venujú kontrolám informačných technológií a prevádzkových technológií
- Je potrebné mať zavedené spoľahlivé opatrenia pre väčšinu z nižšie uvedených kľúčových oblastí
- V prípade nedostatkov v bezpečnostných opatreniach by mali byť tieto nedostatky minimálne a musia byť zdôvodnené



AON

Frekvencia výskytu ransomvéru & vývoj sadzieb cyber poistenia



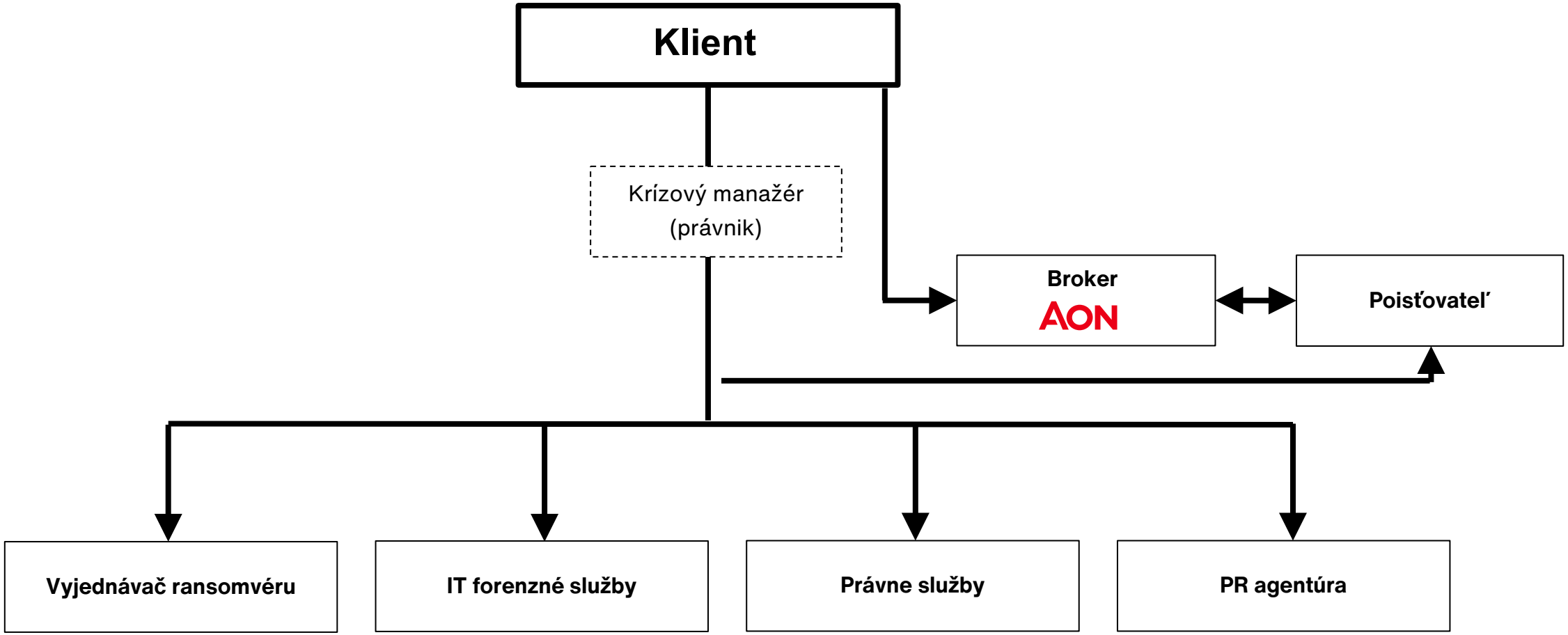
Source: Risk Based Security, analysis by Aon. Data as of 10/1/2024; Claim count development may cause these percentages to change over time

Dopad kybernetického incidentu: S poistením vs bez poistenia

Krytie	S poistením kybernetických rizík	Bez kybernetického poistenia
Náklady na prvú reakciu	Prístup k asistenčnej službe (24/7) v prípade bezpečnostného incidentu Poisťovňa preberá náklady a poskytne krízového manažéra na riadenie incidentu	Strata času pri hľadaní poskytovateľa na reakciu pri incidente Náklady znáša spoločnosť
Náklady na oznámenie & právne náklady	Poisťovňa poskytuje prístup k špecializovaným poskytovateľom v oblasti oznamovania regulačným orgánom a tretím stranám Poisťovňa preberá náklady	Nedostatok určených poskytovateľov, strata času pri hľadaní vhodného poskytovateľa pre oznámenie a právne poradenstvo Mnohé advokátske kancelárie nie sú špecializované na ochranu údajov Náklady znáša spoločnosť
Náklady na styk s verejnosťou (PR)	Poisťovňa poskytuje dedikovanú (PR) agentúru na riadenie celého procesu pre styk s verejnosťou na zmiernenie následkov incidentu. Poisťovňa preberá náklady	Žiadna špecializovaná agentúra pre styk s verejnosťou. Pre spoločnosť môže mať v prípade incidentu veľký dopad na reputáciu
Náklady na forenzné služby	Poisťovňa poskytuje služby forenzného špecialistu na okamžitú reakciu a odborné poradenstvo Poisťovňa preberá náklady	Žiadny prístup k forenzným/odborným službám, pokiaľ nie je uzatvorená zmluva s dedikovaným poskytovateľom forenzných služieb. Náklady znáša spoločnosť
Zodpovednosť za škodu	Poisťovňa kryje nároky na náhradu škody voči tretím stranám vrátane nákladov na obhajobu alebo pokuty od dozorného orgánu	Spoločnosť znáša všetky nároky, pokuty a náklady na obhajobu, ktoré vznikli v súvislosti s incidentom
Prerušenie prevádzky/náklady na obnovu systémov a dát	Poisťovňa uhradí stratu na zisku spôsobenú prerušením prevádzky v dôsledku incidentu, vrátane mimoriadnych nákladov a nadčasov zamestnancov	Majetkové poistenie sa nevzťahuje a vylučuje prerušenie prevádzky z titulu kybernetického incidentu Náklady na prerušenie prevádzky a ušlý zisk znáša spoločnosť

AON

Navrhovaný postup na reakciu pri kybernetickom incidente



AON

Ďakujeme za Vašu pozornosť!

Kontaktujte nás:

LGP
LANSKY, GANZGER, JACKO + PARTNER
RECHTSANWÄLTE / ATTORNEYS

MOORE BDR

DXC TECHNOLOGY

AON