

---

# RIADENIE KYBERNETICKEJ BEZPEČNOSTI VO VZŤAHOCH S TRETÍMI STRANAMI A BEZPEČNOSŤ DODÁVATEĽSKÉHO REŤAZCA



Financované  
Európskou úniou  
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ  
CENTRUM  
KYBERNETICKEJ  
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ  
UNIVERZITA V BRATISLAVE

---

# OBSAH

1. **Úvod:** Prepojený svet a nové riziká
2. **Tretie strany a kybernetická bezpečnosť:** Definície a riziká
3. **Zmluvy s dodávateľmi:** Právne nástroje na riadenie rizík
4. **Strategický imperatív TPRM:** Rozdiel medzi VRM a TPRM, anatómia hrozieb
5. **Životný cyklus TPRM:** Fázy efektívneho riadenia
6. **Technické kontroly a osvedčené postupy:** Praktická implementácia
7. **Híbková analýza a strategické riadenie:** Pokročilé hodnotenie a due diligence
8. **Pokročilé a vznikajúce rizikové domény:** N-té strany, koncentrované riziko a AI
9. **Regulačné rámce a štandardy:** Prehľad kľúčových noriem
10. **Plánovanie reakcie na incidenty:** Koordinácia s tretími stranami
11. **Právne dôsledky a kybernetické poistenie**
12. **Záver a odporúčania pre rôznych používateľov**

---

# ÚVOD

- Prečo je dôležité riadiť bezpečnosť dodávateľského reťazca
- Príklady útokov a ich dopady, poučenia

---

# ÚVOD: PREPOJENÝ SVET A NOVÉ RIZIKÁ

- Organizácie sa dnes spoliehajú na komplexný ekosystém externých partnerov, dodávateľov a poskytovateľov služieb.
- Táto závislosť prináša efektívnosť a inovácie, ale zároveň otvára nové a komplexné vektory kybernetických rizík.
- **Štatistiky ukazujú rastúcu závislosť:**
  - 60 % organizácií spolupracuje s viac ako 1 000 tretími stranami.
  - 71 % hlási nárast počtu dodávateľov za posledné tri roky.
  - 73 % uvádza, že ich tretie strany majú väčší prístup k ich dátam ako pred tromi rokmi.

---

# ÚVOD: SYSTÉMOVÉ RIZIKO A NAJSLABŠÍ ČLÁNOK



- Rast rizika nie je lineárny, vznikajú zložité vzájomné závislosti. Vzájomná prepojenosť systémov pôsobí ako **multiplikátor rizika**.
- Ak je jeden článok v dodávateľskom reťazci kompromitovaný, celý systém je v ohrození.
- **Riziko** už nie je izolované, ale **sa stáva systémovým**, čo môže viesť k rozsiahlym škodám z jedného bodu zlyhania.
- Organizácie musia prejsť od interného zamerania na bezpečnosť k holistickému prístupu „**bezpečnosti ekosystému**“, kde celkovú odolnosť určuje najslabší článok.

---

# ÚVOD: TRADIČNÉ METÓDY UŽ NESTAČIA

- Až 62 % sieťových prienikov pochádza od tretej strany. Tieto útoky sú často úspešné, pretože tretie strany môžu mať slabšie bezpečnostné kontroly.
  - Opakujúci sa vzor: útočníci dôsledne cieľia na "slabších" v rámci dodávateľského reťazca.
- Tradičné, manuálne a periodické metódy hodnotenia rizík už nie sú dostatočné.
- Historicky sa organizácie spoliehali na ročné, manuálne samo-hodnotenia dodávateľov, čo už nie je flexibilné ani škálovateľné.
- Je nevyhnutné **prijat' škálovateľné, automatizované riešenia** a posunúť sa k **nepretržitému monitorovaniu**.

---

# ÚVOD: NESLÁVNE ZNÁME PRÍKLADY ÚTOKOV

Útočníci dôsledne cielia na slabšie bezpečnostné kontroly v rámci dodávateľského reťazca.

- **MOVEit (2023):** Zneužitie zraniteľnosti SQL injection v platforme na prenos súborov postihlo viac ako 130 organizácií, vrátane British Airways a BBC.
- **3CX (2023):** Útok severokórejskej skupiny na aplikáciu pre hlasové a video konferencie postihol vyššie 100 organizácií, vrátane kritickej infraštruktúry v USA a Európe.
- **SolarWinds (2020):** Útočníci vložili zadné vrátka do aktualizácií softvéru Orion, čo viedlo k rozsiahlym únikom dát vo firemných a vládnych organizáciách.
- **NotPetya (2017):** Ransomvér cielený na ukrajinský účtovný softvér spôsobil rozsiahle finančné a operačné škody.
- **Cleo (4/25):** SW na prenos súborov, zraniteľnosť z 12/24, ~60 firiem (aj Hertz) prišlo o dáta

---

# ÚVOD: POUČENIE Z ÚTOKOV

- Opakujúci sa vzor útokov ukazuje, že útočníci preferujú cielenie na slabšie bezpečnostné kontroly v dodávateľskom reťazci.
- Len **reaktívny prístup** po narušení **je nedostatočný**; **proaktívne opatrenia** sú prvoradé na pretrhnutie cyklu útokov.
- Je nutné implementovať bezpečnostný prístup "**shift-left**": zabudovať bezpečnosť do raných fáz životného cyklu spolupráce s dodávateľmi a nepretržite ich monitorovať.
- Zdôrazňuje to kritickú potrebu **zdieľanej zodpovednosti** a spolupráce v celom dodávateľskom reťazci.

---

# TRETIE STRANY A ZMLUVY S NIMI

---

# DEFINÍCIE KLÚČOVÝCH POJMOV

- **TPRM (Third-Party Risk Management):** Systematický proces identifikácie, hodnotenia a zmierňovania rizík, ktoré vznikajú zo spolupráce s externými subjektmi.  
*(zdravie firmy, finančné toky, etika, personálne zabezpečenie)*
- **TPCRM (Third-Party Cyber Risk Management):** TPRM + kybernetické riziká
- **Bezpečnosť dodávateľského reťazca:** Rozširuje koncept TPRM na ochranu IT a softvérových systémov pred hrozbami, ktoré môžu preniknúť prostredníctvom softvéru, hardvéru alebo služieb tretích strán.
- **Tretie strany ...**

---

# TRETIE STRANY: KTO SÚ A PREČO SÚ DÔLEŽITÉ?

**Definícia:** **Tretie strany** sú akékoľvek externé spoločnosti, jednotlivci alebo organizácie, ktoré majú prístup k vašim dátam, systémom alebo sieti.

Príklady:

- Dodávatelia softvéru (Microsoft 365, Google Workspace)
- Poskytovatelia cloudu (AWS, Azure, GCP)
- Konzultanti a externí spolupracovníci
- Marketingové a PR agentúry
- Fyzickí dodávatelia (upratovacie služby)

---

# TRETIE STRANY: AKÉ RIZIKÁ PRINÁŠAJÚ?

Ak má externá firma nedostatočnú ochranu, môže sa stať slabým článkom, cez ktorý útočníci napadnú túto firmu. [Možné dopady](#):

- **Únik dát:** Ak je napadnutý dodávateľ (napr. mzdová agentúra), môžu byť ukradnuté citlivé údaje zamestnancov alebo zákazníkov.
- **Výpadok služieb:** Technický výpadok alebo útok na cloudového poskytovateľa môže spôsobiť nedostupnosť vášho e-shopu alebo firemnej aplikácie.
- **Šírenie malvéru:** Softvér od dodávateľa môže obsahovať škodlivý kód (ransomvér), ktorý sa rozšíri do interných systémov.

---

# TRETIE STRANY: KONCEPT ROZŠÍRENEJ ZODPOVEDNOSTI (1/2)

- Zodpovednosť za bezpečnosť dát sa rozširuje za hranice vlastnej technologickej infraštruktúry.
- **Kľúčový princíp:** Aj keď sa incident stane mimo vašej primárnej IT infraštruktúry, právna zodpovednosť za zabezpečenie riadneho oznámenia postihnutým stranám často stále spočíva na vašej organizácii ako pôvodnom zberateľovi dát.
- **Zásadný omyl:** Predstava, že riziko je možné outsourcovať.

---

# TRETIE STRANY: KONCEPT ROZŠÍRENEJ ZODPOVEDNOSTI (2/2)

- Služby je možné delegovať, ale **zodpovednosť za riziko zostáva plne v rukách pôvodnej organizácie**.
- V prípade úniku dát z tretej strany právna zodpovednosť za oznámenie incidentu často spočíva na vašej organizácii ako pôvodnom zberateľovi dát.
- Organizácie nemôžu jednoducho outsourcovať riziko; musia ho aktívne riadiť, aj keď sú dáta v rukách tretích strán.

---

# ZMLUVY S DODÁVATEĽMI: PRÁVNE BEZPEČNOSTNÉ PÁSY

- Zmluvy sú viac než len dohody o cene; sú to právne "bezpečnostné pásy", ktoré definujú, ako má dodávateľ chrániť vaše dáta.
- Hoci primárna organizácia zostáva právne zodpovedná za úniky dát, robustné zmluvné klauzuly sú kritickým mechanizmom na:
  - Vynútenie bezpečnostných štandardov u dodávateľov.
  - Potenciálne získanie náhrady škody.
- Integrácia právnych a obstarávacích tímov do procesu TP[C]RM je nevyhnutná.

---

# ZMLUVY: KLÚČOVÉ BEZPEČNOSTNÉ KLAUZULY (1/2)

- **Ochrana a dôvernosť údajov:** Jasne definovať, aké dáta dodávateľ spracováva a ako ich bude chrániť (napr. šifrovanie v pokoji a pri prenose).
- **Minimálne bezpečnostné štandardy:** Vynútitel'ná požiadavka na implementáciu kontrol ako MFA, aktuálny antivírus/EDR, správna konfigurácia firewallov a riadenie zraniteľností.
- **Hlásenie incidentov:** Zmluvná povinnosť okamžite informovať o bezpečnostnom incidente v presne stanovenom časovom rámci (napr. do 24 hodín).

---

# ZMLUVY: KLÚČOVÉ BEZPEČNOSTNÉ KLAUZULY (2/2)

- **Právo na audit:** Právo organizácie pravidelne kontrolovať, či dodávateľ dodržiava bezpečnostné štandardy, vrátane požiadaviek na certifikácie (ISO 27001, SOC 2).
- **Riadenie subdodávateľov (Štvrté strany):** Požiadavka na súhlas so zapojením subdodávateľov a prenesenie všetkých bezpečnostných záväzkov na nich.
- **Bezpečné ukončenie spolupráce (Offboarding):** Definovať postupy pre bezpečné vrátenie alebo zničenie všetkých dát a zrušenie prístupových práv.

---

# ZMLUVY: TVORBA ZMYSLUPLNÝCH BEZPEČNOSTNÝCH SLA

- **SLA (Service Level Agreement):** Dohody o úrovni služieb musia definovať **merateľné bezpečnostné ciele a metriky** výkonnosti.
- **Kľúčové prvky bezpečnostných SLA:**
  - **Záruky dostupnosti** (napr. 99,99 %).
  - **Cieľové časy reakcie** na bezpečnostné incidenty podľa ich závažnosti.
  - **Sankcie** alebo kredity za služby v prípade nedodržania.
  - **Časové rámce** na opravu zraniteľností (napr. 72 hodín pre kritické).
  - **Frekvencia** bezpečnostného testovania a podávania správ o súlade.

---

# PRVÁ LÍNIA OBRANY - ĽUDIA

- Každý zamestnanec má dôležitú úlohu pri ochrane organizácie.
- Útoky sa často začínajú sociálnym inžinierstvom, ako je e-mailový podvod, alebo zneužitím slabých hesiel.
- Ľudská chyba alebo náchylnosť na manipuláciu sú hlavnými vstupnými bodmi pre útočníkov.
- Školenie o kybernetickej bezpečnosti pre **všetkých** zamestnancov je nákladovo-efektívnym obranným mechanizmom, ktorý premieňa zamestnancov na aktívnych obrancov.

---

# ZÁKLADNÉ PRAVIDLÁ PRE VŠETKÝCH ZAMESTNANCOV (1/2)

- **Buďte mimoriadne opatrní:** Vždy si dôkladne overte, komu dávate prístup. Ak si nie ste istí, poraďte sa s manažérom alebo IT oddelením.
- **Používajte silné heslá a MFA:** Pre každý účet používajte dlhé, zložité a jedinečné heslá. Kdekoľvek je to možné, vždy aktivujte viacfaktorovú autentifikáciu (MFA).
- **Rozpoznajte phishing:** Dôkladne si overte odosielateľa, neklikajte na podozrivé odkazy a nikdy nestahujte neoverené prílohy.

---

# ZÁKLADNÉ PRAVIDLÁ PRE VŠETKÝCH ZAMESTNANCOV (2/2)

- **Pravidelne aktualizujte softvér:** Aktualizácie často obsahujú dôležité bezpečnostné záplaty. Zanedbanie aktualizácií môže vytvoriť ľahko zneužiteľné "zadné vrátka" pre útočníkov.
- **Zdieľajte informácie len nevyhnutne:** Nezdieľajte citlivé firemné informácie s externými stranami, pokiaľ to nie je absolútne nevyhnutné a máte na to jasné schválenie.

---

# **BONUS: STRATÉGIA**

---

# STRATÉGIA: TPRM VS. VRM – EVOLÚCIA PRÍSTUPU

- **VRM (Vendor Risk Management)**: Základný proces preverovania dodávateľov, zameraný na **zmluvný súlad**. Je to východiskový bod.
- **TPRM (Third-Party Risk Management)**: Širšia a strategickejšia disciplína, ktorá zahŕňa každý vzťah s treťou stranou (partneri, agentúry). Zameriava sa na **odolnosť celého ekosystému**.
- Posun od VRM k TPRM je posunom od činnosti zameranej na právne oddelenie k holistickej stratégii zameranej na **celkovú obchodnú odolnosť**.

---

# STRATÉGIA: ANATÓMIA RIZÍK TRETÍCH STRÁN

Riziká spojené s tretími stranami sú mnohostranné:

- **Kybernetické:** Úniky dát, malvér, neoprávnený prístup.
- **Operačné:** Prerušenie prevádzky v dôsledku zlyhania dodávateľa.
- **Finančné:** Strata príjmov, náklady na zmiernenie škôd.
- **Reputačné:** Negatívny dopad na dôveru zákazníkov v dôsledku incidentu u dodávateľa.
- **Regulačné a súladové:** Pokuty a sankcie v dôsledku nedodržania predpisov dodávateľom.
- **Strategické:** Ohrozenie obchodných cieľov v dôsledku nezosúladených rozhodnutí dodávateľa.

---

# STRATÉGIA: DOMINO EFEKT RIZÍK

- Uvedené kategórie rizík nie sú izolované, ale sú **hlboko prepojené** a často spúšťajú domino efekt.
- **Príklad kaskádového scenára:**
  1. **Kybernetický incident** (ransomvérový útok na dodávateľa) sa stáva...
  2. **Operačným rizikom** (prerušenie služby), ktoré vyvolá...
  3. **Finančné riziko** (strata príjmov) a **riziko súladu** (nesplnenie povinnosti nahlásiť incident podľa DORA/NIS2), čo nakoniec vedie k...
  4. **Reputačnému riziku** (strata dôvery zákazníkov).
- Zrelý program TPRM musí modelovať tieto kaskádové scenáre, aby pochopil skutočný dopad.

---

# **ŽIVOTNÝ CYKLUS TPRM A TECHNICKÉ OPATRENIA**

---

# ŽIVOTNÝ CYKLUS TPRM: PREHLÁD FÁZ

Efektívne TPRM je nepretržitý proces, ktorý zahŕňa celý životný cyklus vzťahu s dodávateľom.

Hlavné fázy:

1. Plánovanie a identifikácia
2. Due diligence a výber
3. Formalizované zapojenie (Onboarding)
4. Hodnotenie rizík a implementácia kontrol
5. Nepretržité monitorovanie
6. Ukončenie a odhlásenie (Offboarding)

---

# ŽIVOTNÝ CYKLUS TPRM: FÁZY (1/2)

## 1. Plánovanie a identifikácia:

- Definovanie kritérií a tolerancie rizika.
- Vytvorenie komplexného inventára dodávateľov, vrátane objavovania "tieňového IT".

## 2. Due diligence a výber:

- Dôkladné posúdenie dodávateľov pred uzavretím zmluvy (bezpečnosť, financie, súlad).
- Použitie dotazníkov, bezpečnostných ratingov, auditov a penetračných testov.
- Klasifikácia dodávateľov podľa kritickosti.

## 3. Formalizované zapojenie (Onboarding):

- Finalizácia zmlúv s podrobnými bezpečnostnými klauzulami.
  - Nastavenie očakávaní a kľúčových ukazovateľov výkonnosti (KPI).
-

---

# ŽIVOTNÝ CYKLUS TPRM: FÁZY (2/2)

## 4. & 5. Hodnotenie rizík a nepretržité monitorovanie:

- Riziko nie je statické; je nutné nepretržite vyhodnocovať bezpečnostné postoje 3. strán.
- Historické manuálne hodnotenia už nie sú dostatočné.
- Automatizované nástroje poskytujú denný prehľad o bezpečnostnej výkonnosti dodávateľa.

## 6. Ukončenie (Offboarding):

- Často prehliadaná, ale kritická fáza.
- Zahŕňa bezpečné ukončenie vzťahu, deaktiváciu účtov, ukončenie tokov dát a bezpečné zničenie firemných dát.
- Overenie vrátenia všetkých aktív a dát.

---

# TECHNICKÉ KONTROLY: RIADENIE PRÍSTUPU (ACCESS MANAGEMENT)

- **Princíp najmenších privilégií (Least Privilege):** Udeliť dodávateľom len minimálny prístup nevyhnutný na vykonávanie ich úloh.
- **Viacfaktorová autentifikácia (MFA):** Vynútenie MFA pre všetok prístup tretích strán je základom.
- **Riadenie privilegovaného prístupu (PAM):** Riešenia, ktoré izolujú, kontrolujú a auditujú privilegované relácie dodávateľov.
- **Just-in-Time Provisioning (JIT/dynamic):** Automatizované poskytovanie prístupových práv len na nevyhnutnú dobu.

---

# TECHNICKÉ KONTROLY: SEGMENTÁCIA A ZRANITEĽNOSTI

- **Sieťová segmentácia:**

- Rozdelenie siete na menšie, izolované zóny (VLANy, subnety).
- Obmedzuje laterálny pohyb útočníkov; ak dôjde k narušeniu jedného segmentu, útok sa nešíri ďalej.
- **Mikrosegmentácia** poskytuje ešte granulárnejšiu kontrolu na úrovni aplikácií.

- **Správa zraniteľností a záplat:**

- Pravidelné skenovanie a prioritizácia záplat na základe rizika.
- Automatizácia procesu záplatovania a zmluvné definovanie lehôt na ich aplikáciu (napr. 72h pre kritické).

---

# TECHNICKÉ KONTROLY: BEZPEČNÁ KONFIGURÁCIA (HARDENING)

Zahŕňa nepretržitú detekciu a nápravu nesprávnych konfigurácií.

- **Audit firewallov:** Kontrola správnej konfigurácie a blokovania nebezpečných portov.
- **Silné politiky hesiel:** Vynútenie komplexnosti, pravidelnej zmeny a jedinečnosti.
- **Šifrovanie dát:** Vynútenie šifrovania dát v kľude (napr. BitLocker) aj pri prenose (TLS/SSL).
- **Riadenie používateľských práv:** Odstránenie nepotrebných administrátorských práv.
- **Zakázanie starších protokolov a nepoužívaných služieb:** Identifikácia a zakázanie protokolov ako Telnet, SMBv1.

---

# TECHNICKÉ KONTROLY: LOGOVANIE A MONITOROVANIE

- Bezpečnostný postoj dodávateľa sa môže zmeniť zo dňa na deň, preto je kontinuálne monitorovanie nevyhnutné.
- **Platformy na hodnotenie bezpečnosti** (napr. Bitsight) demokratizovali schopnosť nepretržitého monitorovania.
- **Zber a analýza logov:** Implementácia robustných systémov na zber logov z aktivít tretích strán.
- **SIEM (Security Information and Event Management):** Centralizácia logov, korelácia udalostí a integrácia s EDR pre komplexný prehľad v reálnom čase.

---

# TECHNICKÉ KONTROLY: BEZPEČNOSŤ API

API sú kritické integračné body a musia byť dôkladne zabezpečené.

- **Silná autentifikácia a autorizácia:** Použitie robustných metód ako OAuth 2.0 alebo JWT.
- **Šifrovanie:** Vynútenie TLS/SSL pre všetku API prevádzku.
- **Validácia vstupu:** Dôkladná validácia a sanitizácia všetkých vstupov na prevenciu injekčných útokov (napr. SQL injection).
- **API Gateway:** Použitie gateway ako jednotného vstupného bodu na aplikáciu konzistentných bezpečnostných politík, riadenie prístupu a detekciu hrozieb.

---

**BONUS:**

**HÍBKOVÁ ANALÝZA, RIZIKÁ, AI, RÁMCE, ...**

---

# HÍBKOVÁ ANALÝZA: POKROČILÉ HODNOTENIE A DUE DILIGENCE

Zahrňa vyhodnocovanie bezpečnostných postupov a zraniteľností každého externého partnera.

## Profilovanie rizík:

- **Bezpečnostné dotazníky:** Používanie štandardizovaných dotazníkov (SIG, CAIQ).
- **Bezpečnostné ratingy:** Využívanie objektívnych, externe overiteľných dát (napr. Bitsight) na denný prehľad o kybernetickom zdraví dodávateľa.
- **Audity a penetračné testy:** Overenie robustnosti bezpečnostných opatrení dodávateľa na mieste.

---

# HÍBKOVÁ ANALÝZA: DOTAZNÍKY SIG VS. CAIQ

Dotazníky sú primárnym nástrojom hĺbkovej kontroly, ale vyplnený dotazník je **začiatkom konverzácie, nie jej koncom.**

Atribút	SIG (Standardized Information Gathering)	CAIQ (Consensus Assessments Initiative Questionnaire)
Primárny účel	Komplexné hodnotenie rizík tretích strán.	Cielené hodnotenie poskytovateľov cloudových služieb.
Rozsah	Široký, 18 domén (kyberbezpečnosť, kontinuita...).	Úzko zameraný na riziká cloudu (virtualizácia, kontajnery).
Cieľový dodávateľ	Akýkoľvek typ, najmä v regulovaných odvetviach.	Poskytovatelia IaaS, PaaS, SaaS.
Použitie	Hĺbkové hodnotenie kritických dodávateľov.	Rýchle a efektívne hodnotenie cloudových dodávateľov.

---

---

# HÍBKOVÁ ANALÝZA: RIADENIE RIZÍK 4. A N-TÝCH STRÁN

- **Riziko n-tej strany:** Vztahuje sa na riziká, ktoré predstavujú dodávatelia vašich dodávateľov (štvrté strany), ich dodávatelia (piate strany) a tak ďalej.
- Tradičné TPRM sa zameriava na priame vzťahy (tretie strany), čo zanecháva **obrovské slepé miesta**.
- Narušenie bezpečnosti u štvrtej alebo piatej strany môže mať **kaskádový domino efekt** smerom nahor v dodávateľskom reťazci.
- Vyžaduje si to mapovanie závislostí a využívanie pokročilých technológií na získanie prehľadu.

---

# POKROČILÉ RIZIKÁ: KONCENTROVANÉ RIZIKO A HYPERSKALÁRI

- **Koncentračné riziko:** Nastáva, keď sa organizácia vo veľkej miere spolieha na jedného alebo malý počet dodávateľov, čím vytvára jediný bod zlyhania.
- Toto je obzvlášť akútne v kontexte cloudu, kde sa obrovské množstvo organizácií spolieha na **AWS, Azure a GCP.**
- Výpadok alebo útok na jedného z nich môže spôsobiť rozsiahle, **systemové narušenie pre celú globálnu ekonomiku.**
- Tento problém presahuje úroveň TPRM a stáva sa záležitosťou **národnej a globálnej ekonomickej bezpečnosti.**

---

# POKROČILÉ RIZIKÁ: MODEL ZDIEĽANEJ ZODPOVEDNOSTI V CLOUDE

Tento model vymedzuje bezpečnostné úlohy medzi poskytovateľom cloudu (CSP) a zákazníkom.

- **CSP je zodpovedný za "bezpečnosť cloudu"** (hardvér, infraštruktúra, virtualizácia).
- **Zákazník je zodpovedný za "bezpečnosť v cloude"** (dáta, konfigurácie, riadenie prístupu).
- Zodpovednosť zákazníka sa mení podľa typu služby: najväčšia je v **IaaS** a najmenšia v **SaaS**.

Doména	On-Premises	IaaS	PaaS	SaaS
Fyzická bezpečnosť	Zákazník	Poskytovateľ	Poskytovateľ	Poskytovateľ
Operačný systém	Zákazník	Zákazník	Poskytovateľ	Poskytovateľ
Aplikácie	Zákazník	Zákazník	Zákazník	Poskytovateľ
Dáta a prístup	Zákazník	Zákazník	Zákazník	Zákazník

---

---

# POKROČILÉ RIZIKÁ: DVOJITÁ ÚLOHA UMELEJ INTELIGENCIE (AI) V TPRM

AI transformuje TPRM, no zároveň prináša nové riziká.

**AI ako nástroj na zlepšenie TPRM:**

- **Automatizovaná hĺbková kontrola:** AI skenuje rozsiahle zdroje dát na identifikáciu varovných signálov.
- **Prediktívne hodnotenie rizík:** ML modely predpovedajú pravdepodobnosť budúceho incidentu.
- **Automatizovaná analýza zmlúv:** NLP algoritmy identifikujú rizikové doložky.

**AI ako nový zdroj rizika od dodávateľov:**

- **Otrava tréningových dát (Data Poisoning):** Útočníci môžu do modelu zaviesť zadné vrátka.
- **Vstrekovanie príkazov (Prompt Injection):** Manipulácia LLM, aby obišiel bezpečnostné kontroly.
- **Únik citlivých informácií:** Modely môžu nechtiac odhaliť dôverné dáta.

---

# REGULAČNÉ RÁMCE A ŠTANDARDY: PREHĽAD

Bezpečnostní špecialisti musia mať hlboké znalosti regulačných rámcov a štandardov.  
Kľúčové rámce zahŕňajú:

- **NIST Cybersecurity Framework (CSF) 2.0**
- **ISO 27001**
- **CIS Critical Security Controls (CIS Controls)**
- **SOC 2**
- **Shared Assessments Framework**
- **Regulácie finančného sektora (napr. DORA)**

---

# REGULAČNÉ RÁMCE: NIST CSF 2.0 A ISO 27001

## NIST CSF 2.0:

- Nová funkcia  
**GOVERN (GV)** kladie explicitný dôraz na riadenie dodávateľských reťazcov.
- Kategória  
**GV.SC (Cybersecurity Supply Chain Risk Management)** podrobne popisuje procesy od stanovenia programu až po ukončenie partnerstva.

## ISO 27001:

- Štandard pre systémy riadenia informačnej bezpečnosti (ISMS).
  - **Príloha A, kontrola 5.19** sa špecificky zameriava na informačnú bezpečnosť vo vzťahoch s dodávateľmi.
  - Vyžaduje riadenie rizík spojených s používaním produktov a služieb dodávateľov.
-

---

# PLÁNOVANIE REAKCIE NA INCIDENTY

Efektívna reakcia vyžaduje štruktúrovaný prístup a koordináciu s tretími stranami.

## **Fázy reakcie na incidenty:**

- Príprava
- Identifikácia
- Obmedzenie (Containment)
- Eradikácia
- Obnova (Recovery)
- Ponaučenie (Lessons Learned)

## **Koordinácia s tretími stranami:**

- Zapojte dodávateľov do plánovania a cvičení.
- Zmluvy musia definovať ich roly, zodpovednosti a protokoly pre oznamovanie.

---

# PRÁVNE DÔSLEDKY A KYBERNETICKÉ POISTENIE

Kybernetické poistenie je kľúčovou súčasťou stratégie riadenia rizík.

- **First-Party Coverage (Pokrytie vlastných nákladov):** Chráni vlastné dáta organizácie, pokrýva náklady na obnovu dát, oznámenie zákazníkovi, stratený príjem.
- **Third-Party Coverage (Pokrytie zodpovednosti):** Chráni pred nárokmi tretích strán, pokrýva náklady na súdne spory, pokuty a penále.
- **Kritická dôležitosť:** Je kľúčové, aby poistná zmluva **explicitne pokrývala kybernetické útoky na dáta organizácie, ktoré sú držané dodávateľmi**. Vaša organizácia bude niesť náklady a právnu zodpovednosť, aj keď incident nastane u dodávateľa.

---

# ZÁVER

---

# ZÁVER: KLÚČOVÉ ZÁVERY

- **Rozšírená zodpovednosť:** Organizácia zostáva právne zodpovedná za dáta, aj keď dôjde k úniku u dodávateľa.
- **Systemové riziko:** Zraniteľnosť v jednom bode môže mať kaskádový efekt na celý ekosystém.
- **Zmluvy ako vynútiteľný nástroj:** Sú kritickým právnym mechanizmom na vynútenie bezpečnostných štandardov.
- **Nepretržité monitorovanie:** Ročné hodnotenia sú nedostatočné; je nevyhnutné pre včasnú detekciu a reakciu.
- **Ľudský faktor:** Zamestnanci sú prvou líniou obrany, ale aj najväčšou zraniteľnosťou.

---

# ZÁVEREČNÉ MYŠLIENKY

Riadenie kybernetickej bezpečnosti vo vzťahoch s tretími stranami nie je jednorazová úloha, ale

**nepretržitá, dynamická a strategická priorita.**

Je nevyhnutné, aby organizácie prijali holistický, proaktívny a nepretržitý prístup k zabezpečeniu celého svojho ekosystému. Iba tak môžu účinne chrániť svoje aktíva, reputáciu a kontinuitu podnikania v čoraz prepojenejšom digitálnom svete.

---

# ODPORÚČANIA PRE ROLY

- **Pre bežného používateľa**
- **Pre administrátora systémov**
- **Pre bezpečnostného špecialistu**

---

# ODPORÚČANIA PRE BEŽNÉHO POUŽÍVATEĽA

- **Bud'te ostražití:** Vždy si overujte požiadavky na prístup k dátam a systémom. Ak máte pochybnosti, overte si to u svojho manažéra alebo IT oddelenia.
- **Základná kybernetická hygiena:** Dôsledne používajte silné, jedinečné heslá a MFA. Pravidelne aktualizujte softvér a bud'te opatrní pri otváraní e-mailov a odkazov.
- **Povedomie o riziku:** Pochopte, že vaša interakcia s externými službami môže ovplyvniť bezpečnosť celej organizácie.

**THINK**

**BEFORE YOU**

click open send install

**NEPODĽAHNI**

**TLAKU**

autorita čas nedostatok  
pomoc reciprocita ...

---

# ODPORÚČANIA PRE ADMINISTRÁTORA SYSTÉMOV

- Implementujte princíp najmenších privilégií: Zabezpečte, aby tretie strany mali len minimálny nevyhnutný prístup.
- Vynúťte MFA a PAM: Implementujte viacfaktorovú autentifikáciu a zvážte riešenia pre riadenie privilegovaného prístupu.
- Segmentujte sieť: Rozdeľte sieť na izolované zóny a obmedzte laterálny pohyb.
- Automatizujte správu zraniteľností a konfigurácie systémov.
- Centralizujte logovanie a monitorovanie (napr. SIEM, EDR) na získanie komplexného prehľadu.
- Zabezpečte API pomocou silnej autentifikácie, šifrovania a monitorovania.

---

# ODPORÚČANIA PRE BEZPEČNOSTNÉHO ŠPECIALISTU (1/2)

- **Vytvorte komplexný program TPRM:** Zaved'te štruktúrovaný životný cyklus TPRM (plánovanie, due diligence, monitoring, odhlásenie).
- **Rozšírte dohľad na 4. strany:** Identifikujte a riad'te riziká, ktoré predstavujú subdodávateľa.
- **Využívajte pokročilé hodnotenia rizík:** Integrujte bezpečnostné ratingy, audity a penetračné testy do procesu due diligence a nepretržitého monitorovania.
- **Zosúladi'te sa s regulačnými rámcami:** Zabezpečte, aby program TPRM spĺňal požiadavky NIST CSF, ISO 27001, SOC 2, DORA atď.

---

# ODPORÚČANIA PRE BEZPEČNOSTNÉHO ŠPECIALISTU

## (2/2)

- **Vypracujte plány reakcie na incidenty so zapojením tretích strán:** Definujte jasné roly, komunikačné protokoly a vykonávajte spoločné cvičenia s kľúčovými dodávateľmi.
- **Optimalizujte kybernetické poistenie:** Zabezpečte, aby poistné zmluvy pokrývali riziká tretích strán.
- **Podporujte kultúru kybernetickej bezpečnosti:** Vzdelávajte a školte všetkých zamestnancov, aby sa stali aktívnou súčasťou obrannej stratégie.

---

# ĎAKUJEM ZA POZORNOST

- Otázky a odpověde