Aktuální potřeby řízení dodavatelského řetězce

Luděk Novák; ISACA Czech Republic

13. – 15. října 2026

ISACA
Czech Republic Chapter

Obsah

Vzpomínka na rok 2005

Podíl úspěšných útoků se zapojením 3. strany

Co už se řeší?

Co by se ještě mělo řešet?

Závěr

ISACA Czech Republic Chapter

Vzpomínka na rok 2005

Do účinnosti vstupovalo v řízení operačních rizik bank
Společnost byla klíčovým dodavatele několika bank

Mělo smysl řešit smlouvy?

Vedení pochopilo potřebu kvalitního řízení informační bezpečnosti
Společnost se systematicky připravila na audity ze strany zákazníků

V roce 2009 úspěšně proběhlo několik dodavatelských auditů

ISACA
Czech Republic Chapter

Podíl úspěšných útoků se zapojením 3. strany

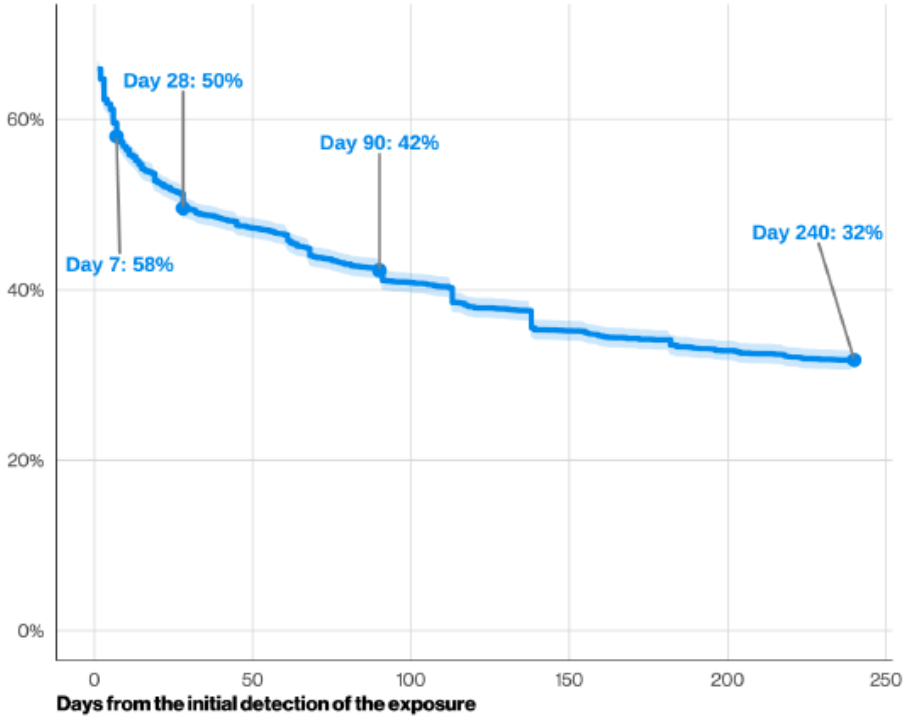


Figure 6. Survival analysis of third-party, cloud-based MFA exposures (n=7,513)

Zdroj: [2026 Data Breach Investigations Report]

Growth in ransomware and third-party breaches continues.

Ransomware grew again to 48% of all breaches, up from 44% from the previous year. However, ransom payments have continued to decline among our dataset, as 69% of ransomware victims didn't pay. The median amount of ransom paid also continues a downward trend: $139,875 in this year's reporting dataset from $150,000 in the previous year.

As organizations increase their reliance on third parties for services and software, their exposure increases, as well, and breaches with third-party involvement have increased by 60% from last year's dataset, reaching 48% of total breaches.

Looking at remediation over time in third-party cloud exposure, only 23% of third-party organizations fully remediated missing or improperly secured multifactor authentication (MFA) on their cloud accounts, with 50% of all findings being resolved within a month.

The third and last measure concerns the involvement of third parties in breaches, and we will dedicate time to discussing it in the next few pages. This metric comes in at 48% this time around, up from 30% last year. That is a 60% increase, after already doubling the year before – quite a trajectory.

This sustained growth has proven impossible to ignore, as many of the year's most high-profile and well-publicized breaches involved multiple third parties. In several of the more notable campaigns, attackers compromised more than one third-party provider at the same time.

ISACA Czech Republic Chapter

Příklad 1: Soulad DORA (2025)

Odběratel: finanční skupina

Nová smlouva podle DORA

- Standardní šablona nepřiměřená rozsahu poskytovaných služeb
- Hodně požadavků mimo poskytovaný rozsah služby
- Neochota vyjednávat / centrála požaduje

Dodavatel: malý IT podnik

- Zajímavá řízená služba v lokálních datových centrech
- Podíl odběratele na obratu cca 0,5 %
- Rozhodnutí vyjednávat s ohledem na rizika
- Plnění všech požadavků DORA mimo realitu obchodního vztahu

Smlouva podepsána, rizika ošetřena

- Zákazník má právo auditu, souhlasí oznámením auditu 3 měsíce dopředu
- Výpovědní doba smlouvy ze strany dodavatele jsou 2 měsíce
- Všichni vypadají spokojeně

ISACA Czech Republic Chapter

Co už se řeší?

Regulace (a právníci) potřebují upravení smluvních vztahů

Dodavatelů je hodně (a bez nich to nejde)

Více se řeší šablony než podstata dodávky a související rizika

ISACA Czech Republic Chapter

Co by se ještě mělo řešit?

Vhodný způsob kategorizace dodavatelů

Výzvy v oblasti zvládání informačních a kybernetických incidentů

Výzvy v oblasti řízení kontinuity činností a služeb IT

Výzvy v oblasti „svobodného“ ukončení partnerství

ISACA Czech Republic Chapter

Vhodný způsob kategorizace dodavatelů (1)

Poskytovatelé řízených služeb / Poskytovatelé řízených bezpečnostních služeb

Systémový integrátoři

Racionální dohled informační a kybernetické bezpečnosti je možný a potřebný

Poskytovatelé cloudových služeb / Poskytovatelé datových center

Telekomunikační operátoři / Dodavatelé energií

Racionální dohled informační a kybernetické bezpečnosti není reálný nebo účinný

ISACA Czech Republic Chapter

Vhodný způsob kategorizace dodavatelů (2)

Kritický poskytovatel

Přímý a podstatný vliv na informační bezpečnost nebo poskytování služeb – např. přístup na úrovni administrátora

Nutné roční přezkoumání plnění závazků včetně revize rizik

Nadstandardní opatrní např. audity, společné nácviky apod.

Důležitý poskytovatel

Méně podstatný vliv na informační bezpečnost nebo poskytování služeb – např. přístup na úrovni koncového uživatele

Základem řízení je pravidelné posuzování rizik poskytovatele

Opatření informační bezpečnosti reagují posouzení rizik

Běžný poskytovatel

Dodavatel nemá podstatný vliv na rizika informační bezpečnosti

Minimalizace činností spojených s řízením poskytovatele

ISACA Czech Republic Chapter

Výzvy v oblasti zvládání informačních a kybernetických incidentů

Řada opatření v oblasti zvládání informačních a kybernetických incident plně neintegruje dodavatele (hlavně poskytovatele)

Doporučen (někde i vyžadován) systematický (vysoce strukturovaný) přístup spojený s ověřováním připravenosti **identifikovat a hlásit** informačních a kybernetických incident (včetně dodavatelů)

Doporučen (někde i vyžadován) systematický (vysoce strukturovaný) přístup spojený s **vyhodnocením** informačních a kybernetických incident a **správným reagováním** (včetně dodavatelů)

Zdroj: VDA ISA 2027 / TISAX

ISACA Czech Republic Chapter

Výzvy v oblasti řízení kontinuity činností a služeb IT

Řada opatření v oblasti kontinuity činností a služeb IT plně neintegruje dodavatele (hlavně poskytovatele)

Doporučen (někde i vyžadován) systematický (vysoce strukturovaný) přístup spojený s ověřováním připravenosti dodavatelů v oblasti kontinuity činností odběratele

- Pravidelná cvičení kontinuity se zapojením dodavatelů, systematické prověřování koordinace

Doporučen (někde i vyžadován) systematický (vysoce strukturovaný) přístup spojený s ověřováním připravenosti dodavatelů v oblasti kontinuity služeb IT

- Pravidelné testování záloh, systematické testování obnovy, systematické prověřování koordinace

ISACA Czech Republic Chapter

Výzvy v oblasti „svobodného“ ukončení partnerství

Pro účinný ukončení partnerství jsou nezbytné potřebné znalosti

- Architektura systému, konfigurační database, znalostní báze, provozní tikety, zdrojové kódy, …

Ukončení partnerství je obtížné a často nemožné, když potřebné znalosti jsou udržovány v prostředí dodavatele

Ukončení partnerství je možné a reálné, když potřebné znalosti jsou udržovány v prostředí odběratele

Zdroj: Petr Hujňák, Exit planning, 2025

ISACA Czech Republic Chapter

Příklad 2: Audit řízení dodavatelů (2024)

Odběratel: vyšší míra regulace

Nálezy u odběratele

- Nesystematické řízení dodavatelů (centrální úroveň / úroveň poskytované služby)
- Nejednoznačné rozdělení odpovědnosti v rámci poskytování služby (odběratel / dodavatel)
- Nebyly prokazatelně sdíleny požadavky na kybernetickou bezpečnost

Dodavatel: Řízená služba provozovaná na zařízeních odběratele, přístupy pro administraci provozovaných systémů

Nálezy u dodavatele

- Neexistence bezpečnostní architektury
- Plány neodpovídaly sjednaným závazkům
- Neplnění závazků ohledně zaškolení
- Neplnění závazků spojených s řízením přístupu a jeho pravidelnou kontrolou
- Nefungovala ani certifikace ISO/IEC 27001 (nekompatibilní rozsah certifikace, neřešeny relevantní regulace, …)

ISACA Czech Republic Chapter

Příklad 3: Sdílení bezpečnostních politik a pravidel s dodavateli (2026)

Odběratel: vyšší míra regulace včetně DORA

Dodavatel: Řízené služby a řízení bezpečnostní služby provozovaná v úzké vazbě na infrastrukturu odběratele, přístupy pro administraci provozovaných systémů

Dodavatel nemá dostupné žádná pravidla a postupy odběratele upřesňující požadavky informační a kybernetické bezpečnosti

Dodavatel nemá dostupné žádná pravidla a postupy odběratele upřesňující klasifikaci incidentů informační a kybernetické bezpečnosti a postupy pro jejich zvládání

ISACA Czech Republic Chapter

Příklad 4: Rizika SLA (2026)

Odběratel: regulace NIS 2 / Dodavatel: řízené služby s SLA (reakce 4 h / fix 24 h)

- Služba realizována v infrastruktuře odběratele
- Politika odběratele předepisuje individuální účty pro administraci
- Dodavateli zbyl jediný účet pro administraci
- Zastupující kolega odešel v roce 2025, účet zrušen bez náhrady

Dobrá zpráva: máme smlouvu vyhovující NIS 2, ale

- Je stanovená SLA vůbec reálná?
- Kdo a jak řídí rizika (odběratel/dodavatel)?

ISACA Czech Republic Chapter

Příklad 5: Fungující odolnost (2026)

Odběratel: Výrobní závod, cca 25 klíčových dodavatelů

- Manažer informační a kybernetické bezpečnosti provádí audit všech dodavatelů každé 2 roky
- Při plánování zohledněny doložená nezávislá ověření (ISO/IEC 27001, TISAX apod.)
- Dobrá znalost místní situace, existujících rizik atd.
- Přímá a osobní komunikace mezi subjekty
- Je zřetelné zlepšování na straně dodavatelů (vědí, že odběratel zase dorazí)

- Změna v souvislosti s NIS 2: vyčlenění MKB mimo útvar IT

ISACA Czech Republic Chapter

Závěr

Účelné řízení dodavatelského řetězce není jen o dobře upravených smluvních vztazích

Je nezbytné dodavatele vhodně kategorizovat

U klíčových dodavatelů je nutný systematický dohled

ISACA Czech Republic Chapter

ISACA
Czech Republic Chapter

Kontakt

Luděk Novák
ISACA Czech Republic
T: + 420 603 248 295
E: novak@isaca.cz

ISACA
Czech Republic Chapter