

Obnova po havárii, kontinuita provozu a reakce na incidenty společnosti ProcessMind

Datum účinnosti: 14. září 2026

Tento dokument poskytuje souhrnný přehled postupů společnosti ProcessMind B.V. pro obnovu po havárii („DR“), kontinuitu provozu („BCP“) a reakci na bezpečnostní incidenty v rámci její cloudové služby. Doplňuje [Bezpečnostní opatření](#), [Zásady hostování SaaS](#), [Dohodu o úrovni služeb](#) a [Dodatek o zpracování údajů](#).

Vysvětluje náš současný přístup a nestanoví samostatné smluvní cíle doby obnovy, cíle bodu obnovy, záruky trvanlivosti údajů, lhůty pro oznámení, úrovně služeb ani standardy odpovědnosti nad rámec toho, co je výslovně uvedeno v příslušné smlouvě, DPA nebo SLA.

1. Cíle a rozsah působnosti

ProcessMind tyto postupy udržuje za účelem:

- ochrany důvěrnosti, integrity a dostupnosti zákaznických dat během mimořádné události
- obnovení kritických komponent produkční služby po selhání systémů pod kontrolou ProcessMind
- zajištění pokračování řízení incidentů, komunikace se zákazníky a provozního rozhodování během výpadků služby
- obnovy po selhání infrastruktury, nasazení, aplikace nebo datové vrstvy pomocí zdokumentovaných postupů a definic infrastruktury spravovaných ve správě zdrojového kódu
- identifikace a posouzení bezpečnostních incidentů, omezení hrozeb, odstranění jejich základních příčin, obnovy dotčených systémů, požadované komunikace a zaznamenání získaných poznatků

Tyto postupy se vztahují na produkční cloudovou službu ProcessMind a na bezpečnostní události týkající se dílčích zpracovatelů nebo cloudových

služeb v rozsahu, v jakém ovlivňují Službu a jejichž prošetření a řešení je v přiměřených možnostech společnosti ProcessMind. Vývojová a testovací prostředí jsou oddělena a nepovažují se za cíle obnovy pro závazky týkající se produkčního prostředí určeného zákazníkům.

2. Strategie odolnosti

2.1 Regionální uspořádání. Produkční služby jsou hostovány v AWS EU (Frankfurt, Německo, eu-central-1). Architektura využívá spravované služby AWS v tomto regionu, které AWS provozuje napříč několika zónami dostupnosti. Cluster Aurora v současnosti používá jedinou instanci zapisovače, takže obnova databáze se opírá o automatizované zálohy a obnovu k určitému časovému okamžiku, nikoli o záložní instanci v rámci regionu. ProcessMind v současnosti neprovozuje druhý aktivní region pro zákaznická data.

2.2 Spravované služby a služby bez serverů. ProcessMind využívá AWS Lambda, Amazon API Gateway, Amazon CloudFront, Amazon Aurora PostgreSQL, Amazon S3, Amazon SQS, Amazon SNS a Amazon CloudWatch. Tím se snižuje závislost na serverech s dlouhou životností spravovaných zákazníkem a podporuje se obnova aplikace a statických komponent opětovným sestavením ze zdrojového kódu.

2.3 Oddělení prostředí. Produkční a vývojová prostředí fungují v oddělených účtech AWS, se samostatnými databázemi a infrastrukturními stacky. Tím se snižuje riziko, že vývojové činnosti ovlivní obnovu produkčního prostředí.

2.4 Monitorování a detekce. Upozornění CloudWatch, dashboardy, upozornění na fronty nedoručených zpráv, centralizované protokolování a syntetické monitorování služeb podporují detekci, třídění a eskalaci incidentů. Potenciální incidenty mohou být zjištěny také prostřednictvím příjmu požadavků na podporu, hlášení zaměstnanců, oznámení dodavatelů nebo jiných podnětů k šetření.

3. Priority obnovy

Obecnými prioritami společnosti ProcessMind při obnově během závažného incidentu jsou:

1. Chránit integritu zákaznických dat a zabránit dalším škodám.
2. Omezit incident a stabilizovat dotčené systémy.
3. Obnovit základní přístupové cesty do produkčního prostředí a kritické workflow.
4. Ověřit fungování služby, integritu dat a monitorování, než bude obnova prohlášena za dokončenou.
5. Informovat o aktuálním stavu, dopadu na zákazníky a následných opatřeních.

Přesné pořadí se může lišit v závislosti na povaze incidentu, včetně toho, zda ovlivňuje integritu dat, přístup zákazníků, asynchronní zpracování nebo podpůrnou infrastrukturu.

4. Postupy obnovy po havárii

4.1 Vyhlášení incidentu a koordinace. Závažná přerušení služeb a bezpečnostní incidenty se třídí podle postupů reakce na incidenty. ProcessMind určí vedoucího incidentu, omezí účast na reakci na oprávněné osoby, posoudí závažnost a rozsah, koordinuje technické pracovníky zapojené do reakce a sleduje opatření k obnově až do vyřešení incidentu nebo snížení jeho závažnosti.

4.2 Omezení dopadu. ProcessMind vynakládá obchodně přiměřené úsilí k zastavení nebo omezení probíhajícího dopadu před zahájením širší obnovy. V závislosti na způsobu selhání mohou opatření k omezení dopadu zahrnovat vrácení nedávných změn, deaktivaci dotčených cest, izolaci nefunkčních komponent, pozastavení zpracování na pozadí během kontrol integrity, odvolání nebo výměnu přihlašovacích údajů či blokování zneužívající činnosti.

4.3 Odstranění příčiny. Po stabilizaci bezprostředního dopadu se ProcessMind snaží odstranit hlavní příčinu nebo přispívající okolnost. To může zahrnovat použití oprav kódu nebo konfigurace, odstranění škodlivých artefaktů, výměnu tajných údajů, obnovení důvěryhodné konfigurace nebo uzavření vystavených přístupových cest.

4.4 Obnova databáze. Aurora PostgreSQL provádí průběžné automatizované zálohování s dobou uchovávání sedm (7) dnů a podporuje obnovu k určitému časovému okamžiku. Pokud selhání na úrovni databáze, poškození dat nebo neúmyslná destruktivní změna vyžaduje obnovu, může ProcessMind obnovit databázi z poslední vhodné zálohy nebo k vybranému časovému okamžiku, ověřit obnovené prostředí a přesměrovat provoz aplikace na obnovenou databázi.

4.5 Obnova objektů a artefaktů. Zákaznické soubory a provozní artefakty se ukládají do Amazon S3. Veřejné verzování je povoleno pro bucket nahraných souborů a buckety zdrojů, aby bylo možné obnovit data po jejich neúmyslném odstranění nebo přepsání. Buckety pro nasazení webových stránek a frontendových komponent se považují za reprodukovatelné artefakty a lze je znovu sestavit ze zdrojového kódu, místo aby se obnovovaly ze záloh.

4.6 Obnova asynchronního pracovního zatížení. Asynchronní cesty zpracování využívají fronty nedoručených zpráv k uchovávání neúspěšných událostí pro účely šetření. Obnova může zahrnovat opakování neúspěšných zpráv, opětovné spuštění logiky zpracování nebo opakované přehrání úloh, pokud příslušné workflow umožňuje jejich bezpečné opětovné zpracování.

4.7 Opětovné sestavení aplikace a infrastruktury. Infrastruktura se spravuje prostřednictvím definic infrastruktury jako kódu, jejichž zdrojový kód je spravován systémem pro správu verzí. Pokud je třeba znovu vytvořit aplikační infrastrukturu nebo statické prostředky, může ProcessMind dotčené komponenty znovu sestavit a nasadit z definic a artefaktů sestavení spravovaných systémem pro správu verzí.

4.8 Ověření před obnovením provozu. Před uzavřením incidentu

ProcessMind ověří stav služby pomocí dostupného monitorování, protokolů, syntetických kontrol a cíleného funkčního ověření a obnoví dotčené funkce pomocí ověřených postupů nasazení, obnovy a správy infrastruktury.

Pokud incident zahrnoval obnovu dat nebo riziko pro jejich integritu, může být provedena další kontrola.

5. Opatření k zajištění kontinuity provozu

5.1 Kontinuita provozu. ProcessMind udržuje zdokumentované provozní postupy, aby během rušivých událostí mohlo pokračovat řešení incidentů, příjem požadavků zákaznické podpory, reakce technického oddělení a rozhodování.

5.2 Komunikace. V případě závažných produkčních incidentů vynakládá ProcessMind obchodně přiměřené úsilí, aby poskytoval aktualizace prostřednictvím kanálů zákaznické podpory a případně na veřejné stránce se stavem služby na adrese processmind.com/status.

5.3 Řízení změn. Ke snížení počtu odvratitelných výpadků a postupnému zlepšování kontinuity se používá vícevrstvý životní cyklus vývoje softwaru s několika nezávislými vrstvami automatizovaného ověřování, řízeným nasazováním, centralizovaným monitorováním a přezkumem po incidentech.

5.4 Bezpečnost během obnovy. Opatření k obnově se provádějí v souladu se stejnými obecnými bezpečnostními zásadami, které platí při běžném provozu, včetně přístupu s nejnižšími nezbytnými oprávněními, zaznamenávání provozních činností, je-li dostupné, a řízeného přístupu k produkčním systémům a datům.

6. Přehled zálohování a ochrany dat

6.1 Zálohy databáze. Automatizované zálohy Aurora jsou šifrovány a uchovávány po dobu sedmi (7) dnů; v rámci této doby uchovávání je k

dispozici obnova k určitému časovému okamžiku.

6.2 Ochrana S3. Amazon S3 zajišťuje vysokou odolnost uložených objektů. Proměnlivé buckety zákaznických dat se spoléhají na odolnost a verzování v primárním regionu. ProcessMind v současnosti pro tyto buckety nepovoluje replikaci S3 mezi regiony.

6.3 Protokoly a diagnostika. Centralizované protokoly, upozornění a telemetrie podporují šetření selhání a ověřování obnovy. Tyto mechanismy podporují činnosti zajišťující kontinuitu, samy o sobě však nejsou prezentovány jako samostatný zálohovací produkt.

7. Identifikace a třídění incidentů

7.1 Počáteční posouzení. Nahlášené události se třídí s cílem určit, zda splňují definici bezpečnostního incidentu, které systémy nebo data mohou být dotčeny, jaký je pravděpodobný rozsah a závažnost a zda je nutné okamžité omezení dopadu. Důkazy se uchovávají způsobem odpovídajícím povaze incidentu a zapojeným systémům.

7.2 Pohotovostní služba a eskalace. ProcessMind zajišťuje pohotovostní pokrytí produkčních incidentů, včetně nepřetržitého pokrytí kritických incidentů (jak jsou definovány ve Smlouvě o úrovni služeb), aby bylo možné incidenty kdykoli potvrdit a roztřídit.

7.3 Dokumentace. ProcessMind dokumentuje podstatná zjištění šetření, opatření v rámci reakce a rozhodnutí o obnově, aby bylo možné po události přezkoumat časovou osu incidentu a následná nápravná opatření.

8. Komunikace a oznamování

8.1 Interní komunikace. ProcessMind koordinuje osoby zapojené do reakce, osoby s rozhodovací pravomocí a kanály podpory, aby technická reakce a komunikace se zákazníky zůstaly sladěny po celou dobu trvání incidentu.

8.2 Oznámení zákazníkům. V případě bezpečnostního incidentu, který vyžaduje oznámení podle DPA nebo příslušných právních předpisů, ProcessMind bez zbytečného odkladu a, je-li to proveditelné, do sedmdesáti dvou (72) hodin od zjištění incidentu informuje dotčené zákazníky. Oznámení obecně obsahují povahu a rozsah incidentu, kategorie dotčených údajů, jsou-li známy, opatření přijatá k omezení dopadu a nápravě incidentu a případná doporučená opatření pro zákazníky.

8.3 Průběžné aktualizace. Pokud incident nadále probíhá nebo se změní podstatné skutečnosti, ProcessMind poskytuje další aktualizace, jakmile jsou k dispozici další ověřené informace. V případě širších přerušení produkční služby může ProcessMind využít také kanály zákaznické podpory a případně veřejnou stránku se stavem služby na adrese processmind.com/status.

9. Testování, přezkum a údržba

ProcessMind tyto postupy přezkoumává alespoň jednou ročně a po závažných incidentech nebo významných změnách architektury, pravidelně testuje příslušné prvky přístupu k reakci a obnově (například obnovu ze záloh, opětovné sestavení nasazení, monitorování, upozorňování a komunikaci při incidentech) a získané poznatky začleňuje do svých postupů v oblasti bezpečnosti, spolehlivosti a kontinuity.

10. Omezení a smluvní hranice

Tento dokument představuje souhrnný přehled a nepopisuje podrobně všechny interní provozní příručky, eskalační cesty, vyšetřovací metody ani kroky při nakládání s důkazy. Nezavazuje společnost ProcessMind k samostatnému návrhu přepnutí mezi regiony, neměnnému uchovávání dat ve všech proměnlivých bucketech ani k nezávislým zárukám RTO/RPO

nad rámec toho, co je výslovně uvedeno v příslušné smlouvě nebo objednávce.

V případě rozporu mezi tímto dokumentem a příslušnou zákaznickou smlouvou, dodatkem o zpracování údajů, smlouvou o úrovni služeb nebo kogentními právními předpisy mají přednost tyto zdroje.