service Operation

Obsah

[service Operation 1](#_Toc179543948)

[úvod 2](#_Toc179543949)

[Primary Breakdown – základné rozdelenie 2](#_Toc179543950)

[Deň zamestnanca v „Téčku“ 3](#_Toc179543951)

[event Management (evm) 3](#_Toc179543952)

[Event Management – úvod 3](#_Toc179543953)

[Event Management – kategórie 4](#_Toc179543954)

[Event Management – príklad mimo IT 5](#_Toc179543955)

[Event Management – procesy 5](#_Toc179543956)

[Incident Management (INM) 6](#_Toc179543957)

[Odhalenie incidentov 7](#_Toc179543958)

[Priorizovanie incidentov 7](#_Toc179543959)

[Major Incidents 8](#_Toc179543960)

[Čiastkové procesy 8](#_Toc179543961)

[Typy zlyhaní a obnovy 9](#_Toc179543962)

[Workaround 9](#_Toc179543963)

[Zhrhnutie 10](#_Toc179543964)

[Resolution (riešenie): 10](#_Toc179543965)

[Solution (náprava): 10](#_Toc179543966)

[problem Management (PRM) 11](#_Toc179543967)

[Problem Management triggers 11](#_Toc179543968)

[Prepojenie Event a Problem Managementu 12](#_Toc179543969)

[Procesné kroky 13](#_Toc179543970)

[The big picture 13](#_Toc179543971)

[Request fulfillment (rff) 14](#_Toc179543972)

[Čiastkové procesy 14](#_Toc179543973)

[Procesné kroky 15](#_Toc179543974)

[Access management 15](#_Toc179543975)

[Čiastkové procesy 16](#_Toc179543976)

[facilities Management 17](#_Toc179543977)

[Funkcie v Service Operation 18](#_Toc179543978)

[IT Operations Control 18](#_Toc179543979)

[Application Management 18](#_Toc179543980)

[Technical Management 19](#_Toc179543981)

[zhrnutie service operation 19](#_Toc179543982)

úvod

Vitajte v Service Operation (prevádzka služby). Ako už názov napovedá, táto časť životného cyklu služby je aktívna vtedy, keď služba, ktorú poskytujeme, má fungovať – prinášať zákazníkom úžitok, pridanú hodnotu.

ITIL, samozrejme, nemôže vedieť, aký druh služby poskytujete, takže vám nemôže skutočne pomôcť s konkrétnymi detailmi poskytovania tejto služby.

Namiesto toho ITIL poskytuje všeobecné osvedčené postupy pre veci, ako je monitorovanie, či služba funguje na očakávaných úrovniach, na riadenie akýchkoľvek prerušení služieb, na vyšetrovanie, prečo k prerušeniam došlo.

Primary Breakdown – základné rozdelenie

Možno si pamätáte, že v časti Service Transition sme zdôraznili Change Management a Configuration Management ako najdôležitejšie procesy – procesy, ktoré by aj začínajúci podnik musel v určitej forme včas implementovať, aby si udržal kontrolu nad svojimi službami.

V Service Operation je oveľa ťažšie určiť jeden alebo dva základné procesy a potom k nim pomaly pridávať ďalšie procesy, pretože tu je všetko prepojené so všetkým ostatným. Z tohto dôvodu má zmysel zavádzať procesy v poradí, ktoré zodpovedá skúsenostiam zákazníkov.

Náš fiktívny **zákazník** alebo **užívateľ** nám môže poslať požiadavku na sprístupnenie existujúcej služby. Táto požiadavka by spustila proces s názvom **Request Fulfilment** (Plnenie požiadaviek). Request Fulfilment je stelesnením princípu „Zákazník je kráľ“: Snaží sa uspokojiť potreby zákazníka, splniť jeho požiadavky.

Keďže zákazník požaduje prístup k službe, ku ktorej predtým nemohol pristupovať, spustí sa proces **Access Management** (správa prístupu), aby bola služba alebo jej časť prístupná. Zvyčajne by to znamenalo, že sa vygenerujú prihlasovacie údaje a poskytnú sa zákazníkovi, alebo že sa jeho používateľský účet pridá do databázy oprávnených používateľov.

Keď sa tak stane, zákazník môže začať túto službu využívať. Kým zákazníci využívajú naše služby, používame **Event Management** na kontrolu fungovania služby. Je všetko v poriadku? Dosahujeme limit našej kapacity? Pokazilo sa niečo? Zisťujeme nejaké pokusy o hacknutie našej služby alebo o to, že sme s ňou urobili niečo nezákonné?

Informácie zhromaždené cez Event Management skôr či neskôr naznačia, že v skutočnosti došlo k nejakému prerušeniu našej služby – možno sa spomalila, alebo možno prestala fungovať úplne. Takéto prerušenia sa nazývajú incidenty a **Incident Management** je proces, ktorý sa pokúša vrátiť službu späť do normálnej prevádzky.

Niekoľko procesov môže naznačovať, že existuje nejaký hlbší, základný **problém**, ktorý ohrozuje našu službu. V takom prípade môžeme použiť **Problem Management**, ktorý je v podstate detektívnou prácou, aby sme zistili, čo je tým hlbším problémom a navrhli trvalé riešenie na jeho odstránenie.

Prostredníctvom všetkých týchto procesov môžeme my, ako poskytovateľ služieb, aj naši zákazníci a užívatelia potrebovať prístup k miestam a oblastiam, kde je umiestnená IT infraštruktúra našej služby. Budeme potrebovať klimatizované kancelárie, fungujúce vodovodné a kanalizačné systémy, elektrinu a osvetlenie a budeme potrebovať naše počítače, aby fungovali, aby sme mali prístup k infraštruktúre a podobne. Aby toto všetko – a ešte viac – fungovalo, sú zavedené štyri procesy: **Facility Management, IT Operation Control, Technical Management** a **Application Management.**

Týchto deväť procesov patrí do prevádzky služieb.

Deň zamestnanca v „Téčku“

V Téčku, keď ráno prídeme do práce, prejdeme cez bezpečnostné turnikety/brány, čo znamená, že Access Management nás pustí, potom sa odvezieme výťahom, ktorý udržiava Facility Management. Pri vstupe do našej kancelárie opäť využívame našu prístupovú kartu, pričom už dýchame prefiltrovaný a príjemne ohriaty alebo ochladený vzduch, ktorý zabezpečuje klimatizácia, ktorú má pod kontrolou Facility Management.

Zapneme svetlá, posadíme sa za stôl a zapneme počítače. Môžeme byť upozornení, že náš systém bol automaticky aktualizovaný na najnovšiu verziu alebo s najnovšími bezpečnostnými záplatami, s láskavým dovolením IT Operations Control a Technical Management.

Takto by sme mohli pokračovať, ale dúfam, že pochopíte, čo sa tu snažíme ukázať: Procesy Service Operation sú skutočne všade, a ako vy alebo zákazník prevádzkujete určitú službu, procesy sa prepínajú medzi aktívnymi a neaktívnymi – pre každú osobu v rôznom čase. Okrem toho, pokiaľ služba funguje normálne, tieto procesy môžu byť takmer neviditeľné alebo nepostrehnuteľné - väčšina ľudí nemyslí na procesy alebo dokonca služby, keď stlačia tlačidlo vo výťahu. Všimneme si to až vtedy, keď sa niečo pokazí, spomalí alebo sa správa nepravidelne.

Pozrime sa teda bližšie na to, ako tieto procesy podporujú bežnú prevádzku služby.

event Management (evm)

Event Management – úvod

Možno trochu prekvapivo začneme s procesom **Event Management**, ktorý bol spomenutý ako tretí proces predtým.

Cieľom Event Managementu je zabezpečiť, aby všetky prvky infraštruktúry, teda všetky konfiguračné položky, boli neustále monitorované. Obrazne povedané, chceme všetkým našim pacientom neustále **kontrolovať pulz**.

Takéto monitorovanie všetkých CIs (konfiguračných položiek) vytvára obrovské množstvo **records** (záznamov) o stave týchto položiek a keďže manuálne kontrolovať každú z nich by nebolo možné, Event management sa ich snaží aj filtrovať a kategorizovať – oddeľovať tie, ktoré vyžadujú zásah človeka od tých, ktoré nie.

Aby sme vysvetlili, ako Event Management funguje a prečo je užitočný, musíme najprv definovať, čo je **Event** (udalosť).

**Event** je akákoľvek **technicky rozlíšiteľná** udalosť, ktorá **by mohla mať dopad** na riadenie IT služby.

Rozložme túto definíciu na jej prvky.

Po prvé, musí byť **technicky rozlíšiteľné alebo rozpoznateľné**. To znamená, že musí existovať jasný a technologicky založený spôsob, ako rozpoznať, že k udalosti došlo. Vzhľadom na skutočnosť, že IT služby sa točia okolo počítačových systémov a že počítačové systémy bežia na elektrinu, zvyčajne to znamená, že elektrina prestala prúdiť cez určitý komponent alebo že sa vygenerovala nejaká digitálna správa.

Po druhé, musí to byť niečo, čo **by mohlo mať dopad na IT službu**. Táto požiadavka naznačuje, že existujú iné udalosti, ktoré **nemôžu** mať dopad. Najjednoduchší spôsob, ako to pochopiť, je zamyslieť sa nad tým, čo sa stane, keď použijete počítačovú myš na spustenie nejakej aplikácie:

Posuňte mouse pointer (kurzor myši) smerom k ikone, ktorá predstavuje aplikáciu, a potom kliknete alebo dvakrát kliknete na ľavé tlačidlo myši, ale mimo ikony. Kedykoľvek sa pozícia myši zmení, hoci len o jeden pixel, teoreticky by sme mohli tento pohyb zistiť a zaznamenať ho, ale keďže akcie v operačnom systéme sa nespúšťajú iba pohybom kurzora myši, pohyb myši zvyčajne nebudeme brať ako event. Na druhej strane, keď dvakrát kliknete na ikonu aplikácie, táto aplikácia **by mohla mať** potenciálne dopad – môže spôsobiť vysoké zaťaženie procesora, zaplniť dostupný úložný priestor údajmi atď. To je dôvod, prečo operačné systémy zvyčajne zaznamenávajú každú spustenú aplikáciu.

Podobne databázový systém zvyčajne zaznamená ako Eventy iba dokončené **database queries** (databázové dotazy), ktoré používateľ alebo aplikácia odošle do databázového systému, a nie jednotlivé stlačenia klávesov.

Ako vedľajšia poznámka, vo **svete počítačových hier** má pohyb myšou a jednotlivé stlačenia kláves zvyčajne význam, takže engine počítačovej hry môže generovať udalosť pre každý pohyb myši a každý stlačený kláves.

Event Management – kategórie

Vo svete IT služieb sú Eventy najčastejšie reprezentované správami – **messages.** Kedykoľvek dôjde k udalosti, komponent, na ktorom sa vyskytla, vygeneruje správu a odošle ju inému komponentu, napríklad operačnému systému, ktorý potom správu spracuje – možno tak, že ju zaznamená do databázy.

Správy sú presne štruktúrované podľa návrhu, čo uľahčuje ich analýzu strojmi alebo programami: Je možné písať analytické programy, ktoré berú každú jednotlivú udalosť, extrahujú z nej informácie a vykonajú nadväzujúce činnosti.

Porovnajte to napríklad s **knihou sťažností**: Keď necháte ľudí napísať svoje sťažnosti, potom ten istý základný problém, ako napríklad „Nedostatok cukru v káve“, môže byť zaznamenaný veľmi odlišnými spôsobmi, ako napríklad:

1. Prečo v mojej káve nebol cukor?!

2. Nabudúce prosím prineste cukor...

3. Táto reštaurácia je na hovno! Žiadny cukor!

Eventy a ich zodpovedajúce správy sú rozdelené do troch hlavných kategórií.

Prvým typom správy je **INFORMATION** (INFORMÁCIA) alebo informatívna správa. Príkladom takejto správy môže byť: „Zariadenie X-Y-Z bolo zapnuté.“ Zvyčajne nie je potrebný žiadny ľudský zásah zo strany poskytovateľa služieb.

Druhým typom správy je **WARNING** (VAROVANIE). Tento typ správy sa generuje, keď komponent infraštruktúry dosiahne vopred definovaný prah. Mohli ste to zažiť, ak vás mobilný telefón informoval, že ste už využili 80 % svojho limitu mobilných dát. Varovanie znamená, že služba je stále funkčná, ale existuje riziko, že ak bude používanie služby pokračovať podľa doterajšieho trendu, môže dôjsť k prerušeniu služby - disk sa môže úplne zaplniť, systém sa môže mať nedostatok pamäte, môže dôjsť k prekročeniu dátového limitu a pod.

Varovné hlásenia sú mimoriadne užitočné pri včasných zásahoch – napríklad keď si všimnete upozornenie na dátový limit, deaktivujete dáta na pozadí, čím sa vyhnete riziku neskoršieho ukončenia bez **akéhokoľvek pripojenia.**

A tretí typ správy sa oficiálne nazýva **EXCEPTION** (VÝNIMKA), niekedy označovaná ako ERROR (CHYBA). Výnimka znamená, že komponent alebo služba nefunguje v rámci očakávaných úrovní – došlo k narušeniu služby. Aby to bolo trochu komplikovanejšie, EXCEPTION nemusí vždy znamenať, že služba nie je dostupná – je tiež možné, že abnormálne úrovne sú, aspoň z pohľadu zákazníka, lepšie, ako sa očakávalo. Z pohľadu poskytovateľa služieb sa však treba zaoberať všetkými výnimkami, pretože neposkytovanie služieb našim zákazníkom, za ktoré si platia, nás vystavuje riziku sankcií alebo straty zákazníka. Bezplatné poskytovanie služby alebo jej časti by zase znehodnotilo túto službu v očiach ostatných zákazníkov.

Event Management – príklad mimo IT

Pozrime sa na Eventy vo svete mimo IT. Ako ste už určite uhádli, opäť sa chystáme navštíviť našu reštauráciu.

Niektoré reštaurácie inštalujú do svojich vchodov buď mechanické alebo elektronické senzory, takže pri otvorení dverí alebo vstupe človeka zazvoní v kuchyni a iných zadných priestoroch zvonček a tým je personál upozornený na tohto nového hosťa.

Pozrime sa, či tento zvonček zodpovedá definícii udalosti:

1. Je to technicky rozpoznateľné? Áno, môžeme mať v kuchyni a iných miestnostiach blikajúce svetlo, ktoré nás upozorní na nového zákazníka.
2. Môže to mať vplyv na poskytovanie našej služby? Určite - buď je to potenciálny zákazník, v takom prípade začneme poskytovať službu, alebo to môže byť niekto so zlými úmyslami, možno lupič alebo zlodej, čo by určite spôsobilo veľké narušenie nami poskytovanej služby ostatným zákazníkom. V každom prípade si musíme uvedomiť, že niekto vstúpil.

Teraz je trochu ťažšia otázka, o aký typ udalosti ide. Je to Information, Warning alebo Exception?

Pokiaľ zvonenie nie je naozaj hlasné a otravné, zrejme môžeme Exception okamžite vylúčiť, nakoľko tento konkrétny človek ešte našu službu nezačal využívať, takže obsluha nemôže byť rušená a ostatných nebude obťažovať zvonenie v našej kuchyni.

Vstup nového návštevníka do našich priestorov je pre nás určite Information, no v prípade reštaurácie je väčšinou potrebná akcia z našej strany. Jedným zo spôsobov, ako sa na to pozrieť, je, že pri príchode nového hosťa mu v hlave začne počítať časový limit a pokiaľ sa im v tomto relatívne krátkom časovom limite dostatočne nevenujeme, rozčúli sa a buď sa sťažujú, alebo odídu. Z tohto pohľadu je to podobné ako zákazník mobilného operátora, ktorý zavolá na našu horúcu linku – ak tento hovor neodpovieme do desiatich minút, zákazník zloží telefón a je nespokojný.

Aké ďalšie Eventy sú možné v reštaurácii? Ďalším príkladom môže byť prázdny pohár na nápoj pred hosťom – to je varovanie, že by sme si mali skontrolovať, či chce doliať.

A ešte jeden príklad: ak sa v kuchyni spustí hlásič dymu, bude to Exception: zákazníci budú musieť opustiť budovu, prídu hasiči a skontrolujú priestory, takže naša služba bude vážne narušená.

Event Management – procesy

V tomto bode už dobre rozumiete tomu, prečo sú udalosti dôležité a prečo ich musíme monitorovať, takže kapitolu môžeme uzavrieť pohľadom na podprocesy Event Managementu.

Prvým z nich je **Maintenance of Event Monitoring Mechanisms and Rules** (Údržba mechanizmov a pravidiel monitorovania udalostí). Ako je v ITIL bežné, robí presne to, čo napovedá jeho názov: Tento podproces zabezpečuje, že všetky nástroje a pravidlá, ktoré používame na monitorovanie, fungujú správne a že keď sa do našej infraštruktúry pridávajú nové komponenty, tieto nástroje a pravidlá sú aktualizované, aby – v podstate – držali krok.

Druhým podprocesom je **Event Filtering and 1st Level Correlation** (filtrovanie udalostí a korelácia 1. úrovne). Názov tohto procesu nie je na prvé počutie úplne jasný, poďme si teda popísať, čo to znamená.

Filtrovanie udalostí znamená, že veľké množstvo udalostí je automaticky analyzované a oddelené na základe vopred definovaných pravidiel; potom sa Information events odfiltrujú, pretože ich možno bezpečne ignorovať. Toto je „Event filtering“ (Filtrovanie udalostí) uvedené v názve procesu. Zostávajúce udalosti Warning a Exception sa prenesú do ďalšieho podprocesu na spracovanie ľuďmi.

Pre toto spracovanie ľuďmi máme **2nd Level Correlation and Response Selection** (koreláciu 2. úrovne a výber reakcie/odozvy). V tomto procese vyškolení operátori interpretujú, čo znamenajú varovné a výnimočné udalosti, a vyberajú, ako sa s nimi najlepšie vysporiadať. V prípade varovných správ sa môžu rozhodnúť ich ignorovať.

Ďalšou najčastejšou reakciou je vytvorenie **incident record** (záznamu o incidente), ktorý potom prechádza procesom **Incident Management.**

Posledným čiastkovým procesom v rámci Event Managementu **je Event Review and Closure** (kontrola a ukončenie udalosti). Tento proces má dva ciele: Zabezpečuje, aby udalosti boli spracované primerane a mohli byť uzavreté, a tiež vykonáva pravidelnú analýzu trendov a vzorcov Eventov. Tieto vzorce môžu naznačovať, že náš návrh infraštruktúry má nejakú chybu, ktorú treba opraviť.

Príklad z histórie Téčka je tento: Po príchode do práce v pondelok ráno storage administrátori objavili Warning, ktoré sa vyskytlo v nedeľu večer a hlásilo, že pevný disk servera je na 98 percent plný. Ale po prihlásení na server videli, že disk je plný len na päťdesiat percent. Varovanie teda ignorovali a sústredili by sa na iné povinnosti. Rovnaká situácia nastala nasledujúci pondelok a pondelok po ňom.

Nakoniec sa niekto rozhodol to ďalej preskúmať, a vtedy odhalil príčinu týchto varovaní: Každú nedeľu večer sa na serveri automaticky spustil zálohovací nástroj, ktorý vytvoril obrovský komprimovaný súbor, ktorý obsahoval presnú kópiu všetkých údajov na disku. Tento súbor bol vytvorený na rovnakom disku, čo znamená, že disk, ktorý bol pôvodne poloprázdny, bude teraz takmer plný. Až keď bol komprimovaný súbor vytvorený, nástroj na zálohovanie ho presunul na externé úložné zariadenie, čím uvoľnil miesto na pevnom disku.

Incident Management (INM)

Event Management môže ako jednu z možných reakcií vytvoriť **incident report** (záznam o incidente). Poďme sa teda pozrieť na **incidenty** a ich riešenie v **Incident Managemente**.

Incident Management incidentov **riadi životný cyklus incidentov,** takže aby sme pochopili jeho dôležitosť, musíme pochopiť, čo je incident.

**Incident je každé neplánované narušenie bežnej prevádzky služby.** Je tiež možné definovať incident ako každý prípad, keď služba funguje mimo plánovaných úrovní prevádzky. Táto druhá definícia zdôrazňuje skutočnosť, že zvyčajne máme pre službu limity tolerancie a až vtedy, keď služba funguje mimo týchto limitov, sa tým zaoberáme.

Asi najzrozumiteľnejším príkladom je rýchlosť sťahovania, pretože väčšina z nás pravidelne sťahuje súbory z internetu alebo siete. Ak váš poskytovateľ internetových služieb sľubuje rýchlosť sťahovania 10 megabajtov za sekundu a vidíte, že sťahovanie v skutočnosti beží rýchlosťou 9 megabajtov za sekundu, vo všeobecnosti chápete, že to môže spôsobiť niekto iný ako váš poskytovateľ služieb. Ak by však rýchlosť bola 20 kilobajtov za sekundu, okamžite by ste si uvedomili, že niečo nie je v poriadku.

Prerušenie normálnej prevádzky bude zvyčajne patriť do jednej z 3 kategórií:

1. V prvej kategórii je služba stále v prevádzke, ale s nižšou rýchlosťou, so zníženou kvalitou, alebo je ovplyvnená nejakým spôsobom, ktorý znepríjemňuje jej používanie. Do tejto kategórie by spadal vyššie uvedený prípad nižšej rýchlosti sťahovania. Ide o **partial disruption** **(**čiastočné narušenie).
2. Druhou kategóriou je **complete disruption** (úplné narušenie), známe aj ako **outage** (výpadok). Služba nie je vôbec dostupná – webová stránka sa nenačíta, mobilné zariadenie hlási „žiadna sieť“.
3. Tretí typ narušenia je typ, ktorý vám zákazníci nemusia vôbec nahlásiť, pretože z ich pohľadu je to výhodné – to je prípad, keď dostanú viac, ako si objednali alebo zaplatili. Môže to byť dočasná chyba alebo výsledok pokusu o hackovanie. Došlo napríklad k úspešným **hacknutiam bankomatov**, ktoré viedli k vyhadzovaniu **bankoviek** zo zariadenia. Ako si viete predstaviť, niektorí zákazníci sa to snažili využiť a bankovky zbierali a snažili sa ich ponechať.

S touto treťou kategóriou nie je spojený oficiálny výraz, ale zákazníci ju môžu označovať ako „free service“ (bezplatnú službu), ak sa im to páči, alebo „sprisahanie“, ak to berú ako dôkaz, že poskytovateľ služby úmyselne znižuje službu, aby si účtoval viac.

Odhalenie incidentov

Incidenty možno odhaliť dvoma spôsobmi: buď **monitorovaním, alebo sťažnosťou používateľov**.

V ideálnom prípade by sme chceli, aby všetky incidenty boli odhalené monitorovacími nástrojmi, pretože to nám dáva príležitosť napraviť incident skôr, ako si to zákazníci všimnú.

Okrem toho, keď prechádzame z klasických technológií na virtualizované systémy, ako sú cloudy, porucha komponentu môže zostať zákazníkovi utajená, pretože službu prevezme a naďalej poskytuje iný prvok infraštruktúry.

Tieto prístupy, niekedy nazývané Dynamic platform or Clouds (dynamické platformy alebo cloudy), sú nevyhnutné pri poskytovaní služieb high availability (vysokej dostupnosti) – služieb, ktoré zdanlivo nikdy nezlyhajú, alebo ak áno, prerušenia majú veľmi krátke trvanie. Dynamické platformy a cloudy sa zvyčajne spoliehajú na redundanciu, ktorá je technickým základom týchto systémov.

Priorizovanie incidentov

Incidenty je potrebné priorizovať, pretože nie všetky incidenty majú rovnaký dopad na zákazníkov a musíme sa vedieť rozhodnúť, ktorý incident riešiť ako prvý a ktorý môže počkať.

Pri stanovovaní priorít sa zvyčajne berú do úvahy dva faktory, ktoré vytvárajú maticu priorít:

1. Prvým z týchto faktorov je **kritickosť služby**, ktorá je ovplyvnená. Služba, ktorá riadi výrobu nových áut a bez ktorej nie je možné vyrábať nové autá, bude považovaná za kritickejšiu ako služba, ktorá umožňuje zamestnancom rezervovať si internú relaxačnú miestnosť.

Vo všeobecnosti platí, že čím bližšie je služba k hlavnej činnosti (core business) zákazníka, tým kritickejšia bude.

1. Druhým faktorom je miera narušenia služieb (level of service disruption). Služba môže byť spomalená, alebo môže byť nedostupná pre malý počet používateľov, alebo môže byť úplne nedostupná, len aby sme vám vymenovali niektoré možné úrovne.

Je dôležité pochopiť, že rovnaký komponent môže mať pre rôznych zákazníkov úplne odlišné kritické vlastnosti. Najlepší spôsob, ako si to predstaviť, je predstaviť si tieto dve zložky: **TELEFÓN a KÁVOVAR**.

Ak vaša spoločnosť **predáva produkty cez telefón**, výpadok vašich telefónov je major disruption (veľkým prerušením) – nebudete môcť obsluhovať zákazníkov. Na druhej strane, ak sa vášmu personálu pokazí kávovar, je to síce drobná nepríjemnosť, no stále môže piť vodu a obsluhovať zákazníkov.

Ale ak **prevádzkujete kaviareň**, výpadok vášho telefónu je len malý problém, niektorí zákazníci si nebudú môcť rezervovať stôl, ale stále môžete svojich zákazníkov obslúžiť. Ak sa však pokazí kávovar, musíte dočasne prestať obsluhovať zákazníkov, pretože nemôžete pripraviť ďalšie šálky kávy.

To je dôvod, prečo by mala byť kritickosť služby alebo komponentu zaznamenaná pre každú CI (konfiguračnú položku) alebo asset (aktívum) nezávisle v CMDB (konfiguračnej databáze).

Kombináciou kritickosti (criticality) príslušnej služby s úrovňou jej narušenia (level of disruption) môžeme zistiť celkovú prioritu takéhoto incidentu. Redundancia môže opäť zabezpečiť, že úroveň prerušenia služby nikdy nebude Total outage (totálny výpadok), čím sa výrazne zníži možnosť **Major Incidentu** – teda incidentu, pri ktorom je kritická služba úplne nedostupná.

Major Incidents

Major Incident znamená **complete outage of a critical service** (úplný výpadok kritickej služby). Ktoré služby sú pre zákazníka kritické, závisia od core business daného zákazníka a musia byť dohodnuté počas vyjednávania zmluvy. Pre automobilku môže byť funkčnosť serverov, ktoré riadia montážnu linku, kritickejšia ako ich emailová komunikácia, zatiaľ čo pre poradenskú spoločnosť alebo tlačovú agentúru je emailová komunikácia životne dôležitá a bez nej jednoducho nemôžu fungovať.

Zmluvy so zákazníkmi zvyčajne špecifikujú, koľko závažných incidentov a koľko hodín výpadku celkovo môže nastať v danom období. Ak poskytovateľ služby nedodá službu v súlade s týmito limitmi, zvyčajne sa uplatnia sankcie, čo samozrejme ovplyvňuje príjmy a môže znamenať rozdiel medzi ziskom a stratou.

Major Incidents predstavujú najvyššiu možnú prioritu a poskytovatelia služieb si zvyčajne stanovujú veľmi prísne časové limity – tak na potvrdenie, že incident existuje, ako aj na obnovenie služby.

Čiastkové procesy

Čiastkové procesy Incident Managementu sú v podstate procesné kroky; väčšina z nich sa stane pri každom incidente a má zmysel opísať ich postupne.

Proces začína zápisom incidentov a kategorizáciou – **Incident Logging and Categorization**. Tu sa vytvorí záznam, ktorý sa časom rozšíri o objavené skutočnosti, navrhované riešenia a ďalšie podrobnosti, zatiaľ však uvádza iba symptómy incidentu. Súčasťou záznamu je **Description** (opis) incidentu. Môže to byť také jednoduché ako „Počítač používateľa sa nespustí“ alebo až také podrobné ako complete error log file (úplný súbor denníka chýb) z aplikácie, ktorá „spadla“.

**Kategorizácia** sa týka rozhodovania o kategórii incidentu, teda či ide o softvérový, sieťový alebo hardvérový problém, či ide o problém s konkrétnou aplikáciou alebo operačným systémom a podobne. To potom pomôže odovzdať incident správnej funkcii (spomeňte si na roly a funkcie), ktorá ho dokáže vyriešiť.

Ak sa zdá, že incident môže byť Major Incident, aktivuje sa vyhradený proces **Handling of Major Incidents** (spracovanie major Incidentov). Inak by prvou akciou, o ktorú sa pokúsite, malo byť **Immediate Incident Resolution By 1st Level Support**  (okamžité vyriešenie incidentu podporou prvej úrovne).

Immediate Incident Resolution By 1st Level Support sa týka činností operátorov hotline alebo operátorov service desk, ktorí majú k dispozícii súbor pokynov na riešenie bežných problémov. Títo operátori nájdu najlepšie usmernenie na základe popisu incidentu a jeho dodržiavaním môžu incident rýchlo vyriešiť.

Ikonická veta z televízneho seriálu „IT Crowd“, ktorá znie: „Skúsili ste to vypnúť a znova zapnúť? je príkladom takého usmernenia, pretože vďaka dizajnu počítačov možno mnohé problémy aspoň dočasne vyriešiť reštartovaním počítača. Aj keď tento prístup nemôžeme odporučiť pre prevádzku Téčka, stále je to užitočný príklad na pochopenie konceptu 1st level resolution.

Ak 1st level support nie je schopný vyriešiť incident, prejde sa na 2nd level support. 2nd level support pozostáva z viacerých špecializovaných funkcií – alebo tímov – s oveľa hlbšími odbornými znalosťami vo svojich odboroch. Tieto funkcie potom využívajú svoje odborné znalosti na vyšetrenie symptómov incidentu, odhalenie root cause (koreňovej príčiny) a vyriešenie incidentu. Toto sa nazýva **Incident Resolution By 2nd Level Support** (riešenie incidentov podporou 2. úrovne) a očakáva sa, že odborníci na 2. úrovni sú schopní vyriešiť akýkoľvek incident vo svojom odbore.

Je dôležité zdôrazniť, že Incident Management sa zameriava na obnovenie normálnej prevádzky. To si však môže vyžadovať výmenu chybného hardvéru, inštaláciu záplaty, premiestnenie zariadení alebo mnoho iných typov zmien. Ak je to tak, Incident Manager spustí **Change Management** požiadaním o Emergency Change a Change sa vykoná v rámci Change Managementu. Po dokončení Change bude requestor of the change (žiadateľ o zmenu) informovaný a práca na incidente bude pokračovať.

Počas celého trvania incidentu je k dispozícii **Incident Monitoring and Escalation** (Monitorovanie a eskalácia incidentov) na pravidelnú kontrolu priebehu všetkých aktívnych incidentov a na ich eskaláciu podľa potreby. Len pre objasnenie možného nedorozumenia spôsobeného kultúrnymi rozdielmi, Eskalácia neznamená niekoho kritizovať, neznamená niekoho trestať a neznamená s niekým rozviazať pracovný pomer. **Eskalácia** znamená prísne upozorniť na problém ďalšie roly, zvyčajne tie, ktoré majú väčšiu rozhodovaciu právomoc alebo majú širší technický dosah. Eskalácia ako taká jednoducho znamená, že niekto s väčšou mocou alebo väčšími skúsenosťami pomôže odstrániť prekážky alebo odhaliť základné príčiny, ktoré pôvodný riešiteľ alebo vyšetrovateľ nedokázal urobiť.

**Pro-Active User Information** (proaktívne informovanie užívateľov) je procesný krok, ktorý varuje užívateľov, že **môžu byť ovplyvnení** incidentom. Takýmto užívateľom to umožňuje pripraviť sa na výpadok služby, čím sa zmiernia negatívne dôsledky a výrazne sa zníži poškodenie dobrého mena poskytovateľa služieb.

Nakoniec, keď je incident vyriešený - to znamená - keď je služba obnovená do normálnej prevádzky, **Incident Closure And Evaluation** uzavrie záznam incidentu **po** kontrole, že bol **skutočne** **vyriešený**, a vykoná niekoľko užitočných činností.

Napríklad v tomto kroku skontrolujeme, čo sa môžeme naučiť z incidentu - objavili sme nejaký spôsob riešenia, ktorý by sa dal znova použiť? Ak áno, kto to bude používať – urobí to 1st level support, alebo je to príliš zložité a vyžaduje si 2nd level support?

Evaluation (vyhodnotenie) môže viesť k vytvoreniu Problem Ticketu. Budeme hovoriť o Problem Managemente ako o ďalšom veľkom procese.

Typy zlyhaní a obnovy

Skôr než dokončíme kapitolu Incident Management, pozrime sa na typy incidentov z pohľadu toho, ako služba zlyhá a ako sa obnoví.

Už sme hovorili o partial disruption (čiastočnom prerušení), ako je napríklad spomalený prenos dát. V prípade čiastočného prerušenia dostávajú používatelia nižšiu kvalitu služby, ale stále môžu dosiahnuť hlavný cieľ - napríklad telefonovať, pozerať video alebo vyrábať autá.

Ďalším možným scenárom je **gradual failure** (postupné zlyhávanie) – v tomto prípade incident začína ako čiastočné narušenie, no postupom času služba stále viac zlyháva, až sa nakoniec stane úplne nedostupnou.

Tak ako môže dôjsť k postupnému zlyhaniu, môže dôjsť aj k postupnej obnove (gradual restoration). Toto je scenár, v ktorom sa služba obnovuje postupne, buď komponentmi alebo zákazníckymi klastrami. Mobilné siete sú opäť dobrým príkladom, pretože v prípade poruchy je ich prvoradé zabezpečiť, aby bolo možné uskutočniť tiesňové volania. Operátori by preto najskôr obnovili funkčnosť **základných telefónnych hovorov**, najmä na čísla tiesňových služieb typu 112 v Európe alebo 911 v USA, a potom obnovili **funkčnosť SMS**, pretože niektorí občania nemôžu volať na tiesňové linky a musia byť schopní odosielať núdzové správy. Až po obnovení týchto náležitostí sa obnovia veci ako prenos údajov.

Workaround

Posledný špeciálny prípad, o ktorom budeme hovoriť, je **restoration with a Workaround** (obnova náhradným, dočasným riešením). **Workaround** je dočasná oprava, ktorá sprístupňuje službu aspoň čiastočne, čím poskytuje poskytovateľovi služby viac času na použitie riadneho riešenia a úplné obnovenie služby.

Workarounds sú veľmi časté počas prírodných katastrof alebo po veľkých nehodách. Napríklad, ak katastrofa poškodí most, armáda môže byť požiadaná, aby postavila pontónový most v blízkosti a doprava je presmerovaná. To umožňuje obnovenie premávky, ale samozrejme pri nižšej rýchlosti a nižšej priepustnosti. Potom môžu inžinieri navrhnúť a postaviť nový most na pôvodnom mieste.

Workarounds zvyčajne majú alebo dodržiavajú **nižší štandard zabezpečenia alebo bezpečnosti** a ako také by sa nemali používať ako trvalé riešenie. Napríklad, ak musí byť budova evakuovaná kvôli požiaru, bezpečnostné turnikety môžu byť deaktivované, čo ľuďom umožní voľne opustiť a neskôr vstúpiť. Keďže žiadny útočník nemohol predvídať evakuáciu, existuje len malé riziko, že by to útočník využil a dostal sa do budovy, ale samozrejme, ak turnikety zostali dlhšie nečinné, riziko zneužitia dramaticky narastá. Pozor, vizuálna kontrola občianskych preukazov nie je taká silná bezpečnostná možnosť ako elektronické skenovanie týchto kariet – deaktivovaná karta vás nepustí cez turniket, ale umožní vám prejsť vizuálnou kontrolou.

Zhrhnutie

Aby sme to zhrnuli, incident je každé neplánované prerušenie služby – akákoľvek neplánovaná odchýlka od bežných prevádzkových úrovní.

Prerušenie môže byť čiastočné alebo úplné, vtedy hovoríme o výpadku služby (**service outage**). Ak dôjde k výpadku kritickej služby, incident sa nazýva **Major Incident** a na jeho vyriešenie sa použije špeciálny proces s názvom **Handling of Major Incidents**.

Cieľom Incident Managementu je riešiť incidenty, teda obnoviť normálnu prevádzku, koordinovane a bez spôsobovania zbytočných negatívnych dopadov. Obnovenie normálnej prevádzky sa nazýva **resolution**, nie **solution** – medzi týmito dvoma pojmami je rozdiel.

### Resolution (riešenie):

Vzťahuje sa na **obnovenie normálnej prevádzky služby** po tom, čo nastal incident. Hlavným cieľom je čo najrýchlejšie uviesť dotknutý systém alebo službu späť do prevádzky s minimálnym narušením pre podnik.

Riešenie môže byť niekedy dočasné (napríklad použitie Workaround) a nemusí úplne vyriešiť root cause problému.

Príklad: Ak dôjde k zlyhaniu servera, resolution môže byť reštartovanie servera, aby bol znova online, aj keď root cause zlyhania ešte nie je identifikovaná alebo vyriešená.

### Solution (náprava):

Vzťahuje sa na **trvalú opravu** root cause problému.

Zameriava sa na odstránenie skutočného problému, ktorý spôsobil incident, a tým sa zabráni jeho opakovaniu.

V Problem Managemente sa náprava zvyčajne vykonáva po identifikácii a analýze koreňovej príčiny.

Príklad: Ak server zlyhá kvôli chybnému hardvérovému komponentu, výmenou hardvéru alebo odstránením konkrétnej príčiny dôjde k náprave.

V skratke:

* **Riešenie (Resolution)**: Obnovuje službu dočasne alebo úplne, ale nemusí riešiť hlavnú príčinu (môže zahŕňať workarounds).
* **Náprava (Solution)**: Opravuje root cause problému, čím sa zabráni jeho opätovnému výskytu a poskytuje trvalé riešenie.

V ITIL v3 je **incident riešený** (resolved), aby sa služba rýchlo obnovila, zatiaľ čo **problém je vyriešený** (solved), aby sa zabránilo opakovaniu incidentov.

Incidenty môže riešiť 1st level support, ktorý je vhodnejší pre svoju rýchlosť a nižšie náklady, alebo 2nd level support, ktorý vo všeobecnosti rieši len neobvyklé alebo zložité incidenty, pre ktoré nie je možné pripraviť jednoduché pokyny.

Ak si riešenie incidentu vyžaduje **zmenu konfigurácie infraštruktúry**, ako je výmena chybného hardvéru, inštalácia softvérovej opravy alebo obnovenie databázy zo zálohy, spustí sa Change Management, aby sa zmena vykonala.

A ak **root cause** (koreňová príčina) incidentu nie je známa alebo objavená počas práce na ňom, spustí sa Problem Management, aby sa zistila root cause, ako sa dozvieme v ďalšej kapitole.

problem Management (PRM)

Vieme teda, že incidenty sú narušenie služieb. Všetky narušenia majú root cause (koreňovú príčinu), ale táto root cause nemusí byť zjavná. Na odhalenie root cause a ich dlhodobých riešení máme Problem Management.

Problem Management je, obrazne povedané, **vyšetrovanie miesta činu (crime scene investigation of ITIL)** ITILu. Aby sme úplne pochopili, ako to funguje, pozrime sa najprv na terminológiu.

Hlavným pojmom je **problém**. Problém je **root cause** (koreňová, základná príčina) skutočného alebo potenciálneho incidentu. Pri prvom zaznamenaní problému v **Problem Record** zvyčajne nie je známa root cause.

*Naším cieľom preto bude odhaliť a podrobne opísať hlavnú príčinu incidentu.*

Pre objavené a opísané hlavné príčiny chceme vyvinúť **Workaround – dočasnú opravu**, ktorá čiastočne obnoví službu a poskytne nám viac času na dosiahnutie trvalého riešenia.

Keď je hlavná príčina spárovaná s riešením, stane sa známou chybou – **known error.**

Na zhromažďovanie známych chýb ITIL definuje **Known Error Database, alebo K-E-D-B.**

Ak Workaround nie je potrebný, pretože incident sa dá vyriešiť rýchlo, Problem Management môže vytvoriť **Incident Model** – návod, ako vyriešiť incidenty s touto danou root cause krok za krokom.

Rýchla rekapitulácia pred pokračovaním: Problem record zvyčajne začína ako záhada, niečo ako „Prečo služba zlyhala? Čo to spôsobilo?" Potom sa premení na known error with a workaround, kým skúmame a vyvíjame spôsoby, ako čeliť základnej príčine.

Teraz pre každý z týchto výrazov – Problem, Known Error a Workaround, ITIL definuje aj variant **Suggestion** (návrh) – **Suggested Problem, Suggested Known Error a Suggested Workaround**. Toto sú, ako už názov napovedá, návrhy na zadanie nového záznamu tohto špecifického typu do príslušnej databázy. Ako vždy, ITIL nepredpisuje, ako sa to robí, takže je možné realizovať tieto **Suggestions** ako status alebo flag každého záznamu. Problem record môže mať napríklad pole označené „Status“ s možnými hodnotami **Suggested problem, Accepted problem, Described Root Cause, Described Known Error, a Closed Problem** (Navrhnutý problém, Prijatý problém, Popísaná hlavná príčina, Popísaná známa chyba a zavretý problém) – je to výlučne na rozhodnutí poskytovateľa služieb.

Problem Management triggers

Problem Management **riadi životný cyklus všetkých problémov**.

**Cieľom** je zabrániť incidentom, a ak to nie je možné, potom minimalizovať dopad incidentov.

Aby sme pochopili vplyv Problem Managementu, pozrime sa najprv na to, aké situácie ho môžu spustiť.

1. Prvý spôsob, ako sa Problem Management spustí, je, keď dôjde k Major Incidentu. Keď sa to stane, je Problem Management povinnosťou – pretože úplné výpadky kritických služieb sú také zničujúce a tak ohrozujúce dôveru zákazníkov v poskytovateľa služieb, že je povinnosťou poskytovateľa služieb zabezpečiť, aby sa to už neopakovalo.

To je dôvod, prečo sme v procese Incident Management spomenuli, že pre Major Incidents máme krok **Handling of Major Incidents** a ako súčasť toho musí byť vytvorený Problem record, ktorý spustí Problem Management.

1. Druhým spúšťačom Problem Managementu sú incidenty, *ktorých hlavnú príčinu nepoznáme*. Aj keď incident nemá vážny dosah, skutočnosť, že nevieme, prečo k nemu došlo, musí spustiť vyšetrovanie.

Príklad mimo IT: Ak niekto vypije priveľa alkoholu a na druhý deň ho bolí hlava, bolesť hlavy si pravdepodobne vysvetlí alkoholom. No ak niekoho zrazu začne bolieť hlava a nevie zistiť prečo, návšteva praktického lekára je rozumná vec, pretože môže odhaliť nejaký hlbší problém a prinajmenšom navrhne, ako pacientovi upraviť stravu alebo aktivity.

Ak sa teda nedôležitý počítačový systém začne reštartovať bez akéhokoľvek viditeľného dôvodu, vyšetrovanie môže odhaliť, že vo vnútri je príliš veľa prachu, čo spôsobuje prehrievanie, alebo že mu dochádza miesto na odkladanie na systémovej jednotke. Bez vyšetrovania sa to možno nikdy nedozvieme, a preto nemôžeme zabrániť opakovaniu takéhoto incidentu.

K tomuto druhému spúšťaču treba pridať ešte jednu vec: Špeciálny variant je, keď nevieme, ako vyriešiť incident. Predpokladom je, že ak neviete, ako vyriešiť incident, pri ktorom zdanlivo poznáte hlavnú príčinu, skutočná príčina je hlbšia a stále ste ju nenašli.

1. Tretím dôvodom na spustenie správy problémov sú **recurring incidents (opakujúce sa incidenty)**. Aj keď poznáme hlavnú príčinu nejakého incidentu, ak sa tento incident stále opakuje, mali by sme vynaložiť úsilie, aby sme sa ho zbavili, inak budeme naďalej tráviť čas riešením incidentov a z dlhodobého hľadiska to bude nákladnejšie. Okrem toho, ak si tento incident všimne zákazník, potom bude tento zákazník naštvaný a môže stratiť dôveru v našu schopnosť poskytovať služby vysokej kvality.
2. A posledným dôvodom na spustenie Problem Managementu je, ak sa dozvieme o **potenciálnom incidente**. To je bežné v prípade **security** **vulnerability** (bezpečnosnej zraniteľnosti), ktorá môže byť nahlásená skôr, ako ju môžu zneužiť útočníci. V takom prípade je cieľom Problem Managementu nájsť najlepší spôsob, ako opraviť zraniteľnosť na všetkých potenciálne postihnutých systémoch.

Tieto štyri dôvody možno zhrnúť pomocou výrazov **MAJOR, UNKNOWN, REPEATED, VULNERABLE**. Toto nie je terminológia ITIL, ale ak si pamätáte tieto štyri slová, tieto štyri typy incidentov, malo by vám to pomôcť zrekonštruovať štyri spúšťače pre Problem Management. Problem records – alebo tickets – otvárame, keď dôjde k závažným incidentom, keď nepoznáme hlavnú príčinu, keď sa incidenty opakujú alebo keď sme informovaní o bezpečnostnej zraniteľnosti.

Ako sme už povedali, problém je root cause incidentu – existujúceho alebo potenciálneho. V určitom bode sa root cause zmení z neznámej na známu - z tajomstva, ktoré si vyžaduje detektívnu prácu, na inžiniersku úlohu opraviť rozbitý prvok.

Preto by nemalo byť prekvapením, že každá z týchto fáz si môže vyžadovať iný typ experta – napríklad čítanie podrobných protokolov všetkého, čo sa stalo v databázovom systéme, čo by mohla byť detektívna práca, je úplne odlišné od písania databázového skriptu, ktorý zmení konkrétne nastavenie alebo aktualizuje všetky databázy, čo môžu Workaround alebo permanent solution (trvalé riešenie) vyžadovať.

Z tohto dôvodu by Problem Manager nemal váhať a priradiť vhodných odborníkov, zvyčajne viacerých, na jeden Problem Record – niekoho, kto bude analyzovať a odhalí hlavnú príčinu, a niekoho, kto vyvinie workaround alebo trvalé riešenie. Bežnou chybou je myslieť si, že niekto, kto incident nahlásil alebo vyriešil, je tiež schopný odhaliť jeho root cause a vyriešiť ju. Môže to tak byť, ale netreba to brať ako samozrejmosť.

Prepojenie Event a Problem Managementu

Pamätáte si, keď sme hovorili o Event Managemente? Existujú tri typy udalostí – najkritickejšie udalosti sú EXCEPTIONS a signalizujú, že služba alebo jej komponent nefunguje normálne. Druhým typom sú udalosti WARNING, ktoré indikujú, že služba alebo komponent dosiahli preddefinovaný prah, takže ak trend používania alebo prevádzky pokračuje, daná služba alebo komponent môže dosiahnuť stav EXCEPTIONS.

Hovorili sme však aj o udalostiach typu INFORMATION bez vysvetlenia, prečo sú užitočné.

Problem Management je jedným zo súvisiacich procesov, kde sú udalosti typu INFORMATION mimoriadne užitočné – pretože tieto **informačné** správy vytvorené alebo zaznamenané Event Managementom sú v podstate vodítkami pre detektíva, ktorý vyšetruje root cause.

Bez **informačných** typov správ by sme v event log (protokole udalostí) počítačového systému videli iba „10:30:25 – Server sa vypína z dôvodu nedostatku pamäte“.

Neexistoval spôsob, ako zistiť, čo naplnilo túto pamäť.

Ale vďaka **informačným** správam by tento denník udalostí obsahoval aj tieto položky:

„10:27:15 – používateľ ADMIN prihlásený“

"10:28:40 – Používateľ ADMIN spustil vírus dot exe"

A až po týchto dvoch záznamoch by sme videli chybové hlásenie o nedostatku pamäte. Je zrejmé, že to nám hovorí oveľa viac, teraz vieme, koho sa máme opýtať, ktorú aplikáciu skontrolovať a ako zabrániť tomu, aby sa tento incident opakoval.

Procesné kroky

Na záver kapitoly o Problem Managemente sa pozrime na jednotlivé kroky procesu.

Život jedného problému zvyčajne začína, keď nejaký iný proces nahlási jeho existenciu. Môže to byť cez **Suggested new Problem** (Navrhovaný nový problém) alebo priamo z Incident Managementu. Keď je problém nahlásený, **Problem Categorization and Prioritization** (kategorizácia problémov a priorizovanie) zaisťuje, že Problem record popisuje technologickú oblasť, ktorej zodpovedá, ako je operačný systém, aplikácie alebo špecifický hardvér, a že mu je priradená priorita. Logika určovania priorít je rovnaká ako v prípade incidentov – s obmedzenými zdrojmi musíme byť schopní vybrať, ktoré problémy je potrebné riešiť súrne a ktoré môžu počkať.

Po správnom zaznamenaní, kategorizácii a stanovení priorít je **Problem Diagnosis and Resolution** (diagnostika a riešenie problémov) fázou, ktorá odhalí root cause, vyvinie Workaround alebo trvalé riešenie a prípadne odošle žiadosť Change managementu na implementáciu tohto riešenia. Je bežné, že tento krok trvá niekoľko týždňov reálneho času, rovnako ako detektívne vyšetrovanie trestného činu môže byť časovo náročná činnosť.

Problémy sa zvyčajne končia fázou **Problem Closure and Evaluation** (uzavretím a vyhodnotením problému), pri ktorom sa Known Error Database aktualizuje o Known Error a po uistení sa, že príslušný incident bol vyriešený, možno záznam uzavrieť. Ak bola na implementáciu riešenia spustená Change z Problem Managementu, tento krok sa uskutoční až **po** úspešnej implementácii zmeny.

V procese sú k dispozícii ďalšie dva kroky. Prvým z nich je **Major Problem Review** (preskúmanie závažného problému), v ktorom zisťujeme, či bol Major Problem skutočne natrvalo vyriešený. Major Problems sú problémy pre Marjor Incidents alebo pre opakované incidenty s vysokou prioritou. Logika Major Problem Review spočíva v tom, že možno bolo potrebné opraviť, upgradovať alebo vymeniť viacero systémov, alebo že bolo potrebné vykonať veľa zmien, takže je potrebné ďalšie overenie, aby ste sa uistili, že riešenie je skutočne trvalé.

A nakoniec, **Proactive Problem Identification** (proaktívna identifikácia problémov) je krok, ktorý identifikuje a rieši problémy skôr, ako sa incidenty vyskytnú, alebo skôr, ako sa zopakujú v prípade opakovaných incidentov. Vo všeobecnosti je Proactive Problem Identification znakom vyspelosti služby, pretože poskytovateľ služieb presúva niektoré zdroje od vývoja nových funkcií alebo od zvyšovania podielu na trhu smerom k stabilite a dostupnosti služby.

The big picture

Aby ste si upevnili vaše porozumenie, pozrime sa ešte raz na skupinu vzájomne súvisiacich procesov, o ktorých sme hovorili:

Ako poskytovateľ služieb prevádzkujeme Configuration Items, ktoré sú všetky riadené Service Asset and Configuration Managementom.

Tieto assets (aktíva) sú – dúfajme – všetky monitorované a Event Management zhromažďuje udalosti alebo **správy**, ktoré označujú stav všetkých aktív. Niekedy správy indikujú možné alebo skutočné prerušenie služby, kedy sa Incident Management pokúsi obnoviť normálnu prevádzku. Ak má incident neznámu root cause, alebo ak bol dostatočne závažný na to, aby ohrozoval našu povesť, **Problem Management** to vyšetrí a navrhne riešenie, ktoré riziko tohto incidentu eliminuje.

A ak Incident Management alebo Problem Management potrebujú v rámci riešenia zmeniť konfiguráciu aktív, potom túto Change implementuje Change Management. Aktualizovaná konfigurácia sa potom zaznamená pomocou Service Asset and Configuration Management.

Request fulfillment (rff)

Request Fulfillment (plnenie požiadaviek) je presne to, čo názov napovedá: Proces, ktorý plní požiadavky na služby. Tieto požiadavky sú zvyčajne jednoduché zmeny - Changes, ako je resetovanie hesla alebo naplánovanie automatického štandardizovaného prehľadu.

Historicky sa tieto Requests vyvinuli z incidentov. Ak túto myšlienku obmedzíme len na skutočne jednoduché situácie, ako je zablokovaný prístup k vášmu účtu alebo nemožnosť nainštalovať softvér, môžeme vidieť, že rovnakú situáciu možno považovať buď za incident, alebo za žiadosť.

Na vysvetlenie: Ak sa nemôžete prihlásiť do svojho systému, pretože ste zabudli heslo, potom z vášho pohľadu služba nefunguje. Z pohľadu služby však funguje perfektne – dovnútra vpustí len niekoho, kto pozná heslo, a keďže ste heslo zabudli, nemali by ste byť vpustení. Podobne, ak si nemôžete do pracovného počítača nainštalovať aplikáciu, môže sa vám zdať, že máte zablokované plné používanie počítača, ale takúto reštriktívnu politiku definoval správca a z jeho pohľadu je všetko presne tak, ako má byť. Z tohto dôvodu by bolo nespravodlivé nazývať to incidentom, ak prihlasovacia obrazovka skutočne funguje presne tak, ako by mala, takže namiesto použitia Incident Managementu na resetovanie používateľských hesiel ITIL poskytuje Request Fulfillment.

Čiastkové procesy

Request Fulfillment má tiež podobnosť s Change Managementom, najmä so Standard Changes.

Používatelia zvyčajne odosielajú žiadosť o službu, ktorá je potom zaznamenaná a kategorizovaná.

K dispozícii sú **Request Models** s jasnými pokynmi krok za krokom pre Request Operatora. Rovnako ako v prípade Change Models sú Request Models vopred schválené v tom zmysle, že nikto nemusí kontrolovať platnosť alebo bezpečnosť krokov a jediné povolenie alebo overenie sa týka identity Requestora (žiadateľa) – inými slovami, má táto osoba naozaj právo použiť takúto žiadosť?

Celý proces je pomerne priamočiary a je rozdelený do piatich podprocesov, čiže krokov, z ktorých dva bežia neustále na pozadí a tri z nich sa vykonávajú pre každú požiadavku v poradí.

Proces **Request Fulfillment Support** zabezpečuje, že nástroje a potrebné know-how a samotný proces sú efektívne a účinné. Väčšina z nás má skúsenosti so Service Portals, kde môžeme požiadať o všetky druhy služieb, od premiestnenia pracovného stola až po zmeny osobných údajov alebo dočasné miestne administrátorské práva pre naše počítače. Niektoré z týchto portálov dokonca obmedzujú, kto môže o ktorú službu požiadať, čo je presne jeden zo spôsobov, ako vykonať overenie alebo autorizáciu spomínanú vyššie – ak nástroj neumožní bežnému zamestnancovi o niečo požiadať, potom to zabezpečí, že iba manažér alebo asistent môže o to požiadať.

**Request Monitoring and Escalation** (Monitorovanie požiadaviek a eskalácia) zaisťuje, že existujúce požiadavky sú pravidelne kontrolované a že žiadnej z nich nevyprší alebo neprekročí očakávaný čas vykonania alebo doručenia – napríklad 4 hodiny na obnovenie hesla alebo päť dní na nový preukaz totožnosti. Tento proces sa tiež postará o všetky eskalácie, napríklad keď žiadateľ nie je spokojný s riešením.

To boli dva dlhodobé, zastrešujúce procesné kroky, ktoré sú vždy aktívne.

Procesné kroky

Keď používateľ odošle požiadavku na službu, spracujú ju tri kroky procesu.

Celkom logicky musí byť požiadavka **Logged and Categorized** (zaznamenaná a kategorizovaná). Vďaka moderným počítačovým systémom, ktoré sa na to bežne používajú, sa to zvyčajne vykonáva ako súčasť samoobslužných akcií žiadateľa - keď vyplní konkrétnu šablónu žiadosti, šablóna už vie, o akú kategóriu žiadosti ide, takže tento krok môže byť v podstate okamžitá.

Druhým krokom je **Request Model Execution** - operátor použije správny Request Model a krok za krokom vykoná všetky akcie potrebné na splnenie požiadavky. Prvými krokmi sú zvyčajne overenie alebo autorizácia, ako je zavolanie žiadateľovi a kontrola, či skutočne chce nové heslo alebo novú identifikačnú kartu, a keď je to úspešné, všetky ostatné kroky sa vykonajú.

Pravdepodobne máte skúsenosť so žiadosťou o obnovenie hesla na nejakej voľne dostupnej webovej stránke. Keďže zavolať vám by bolo cenovo nedostupné, namiesto toho používajú potvrdenie e-mailom – to zaisťuje, že žiadosť môže potvrdiť iba aktuálny používateľ e-mailovej adresy priradenej k danému účtu, čo možno interpretovať ako potvrdenie, že daná osoba má skutočný záujem o obnovenie hesla. Sekundárnou výhodou tohto prístupu je, že ak by sa útočník pokúsil obnoviť heslo, legitímny používateľ je o takomto pokuse informovaný touto žiadosťou o potvrdenie.

Nakoniec, keď je model požiadavky úplne vykonaný, musíme skontrolovať, či bol skutočne úspešný. **Request Closure and Evaluation** (uzavretie a vyhodnotenie požiadavky) je krok, v ktorom vykonávame kontrolu kvality. To nielen skontroluje, či je používateľ spokojný so spôsobom, akým bola jeho požiadavka splnená, ale v tomto kroku zhromažďujeme aj všetky užitočné informácie pre budúce vylepšenia procesu alebo služby. Jedným z príkladov je požiadať používateľa o spätnú väzbu, napríklad keď vás internetový obchod požiada, aby ste ohodnotili svoju spokojnosť s tovarom, ktorý ste si kúpili, aj so službou, ktorú ste od obchodu dostali. Ak počas určitého obdobia obchod zistí, že mnohí ľudia hodnotia dodacie lehoty ako zlé, môže to viesť k úpravám doručovacej služby. Podobne, ak sa mnohí používatelia sťažujú, že online šablóna na žiadosť o obnovenie hesla je mätúca, pravdepodobne to povedie k zmene tejto šablóny.

Typický postup plnenia požiadaviek v organizácii poskytovateľa služieb je taký, že Service Desk prijíma, zaznamenáva a kategorizuje všetky požiadavky (**logs and categorizes**) a zvyčajne vykonáva (**executes**) aj jednoduchšie požiadavky, ako je resetovanie hesla. Zložitejšie požiadavky alebo požiadavky, ktoré si vyžadujú špecializované vybavenie – ako napríklad tlačiareň identifikačných kariet – sa prenesú do **Service Request Fulfillment Groups** (skupiny pre plnenie požiadaviek na služby), čo sú zvyčajne 2nd Level Teams, ktoré potom vykonajú príslušný **model.**

Záverečná poznámka týkajúca sa splnenia požiadaviek – pretože tento proces je v podstate ľahšou verziou Change Managementu pre Model Changes, požiadavky sa plnia a vykonávajú priamo v rámci Request Fulfillmentu; inými slovami, nevytvárajú sa žiadne Change Records a neodosielajú sa do Change Managementu. V tom rozdiel oproti Incident Managementu, kde sa zmeny konfigurácie musia realizovať prostredníctvom Change Managementu.

Access management

Ak je Request Fulfillment tou rozprávkovou krstnou mamou, ktorá plní naše želania, potom Access management je nebezpečný troll, ktorý stráži most a kladie záludné otázky.

Dobre, možno to nie je najlepšia analógia, každopádne, pozrime sa bližšie na **Access management** (správu prístupu).

Cieľom Access managementu (správy prístupu) je zabezpečiť, aby autorizovaní používatelia mohli službu plne využívať, zatiaľ čo ostatní ju nemôžu používať vôbec. Niekedy sa namiesto názvu Access management môžu použiť názvy **Rights Management** alebo **Identity Management**.

Pre osvieženie pamäte – v časti Service Design sme hovorili o **Information Security Management**. Tento proces definuje politiky alebo pravidlá pre prístup k určitým informáciám. A zvyčajne pre každú politiku definuje **named priviledge** (pomenované privilégium) alebo **right** (právo), ktoré bude túto politiku reprezentovať.

Access Management potom prevezme tieto definované práva - a ich sprievodné politiky - a implementuje ich alebo vykoná.

Information Security Management môže napríklad definovať úlohu náborového špecialistu, ktorý má prístup k osobným informáciám uchádzačov o zamestnanie. A keďže informácie sú uložené v nástroji, ktorý by sa mohol nazvať Hiring Tool, potom musí Access Management zabezpečiť dve veci: Po prvé, že každý náborový pracovník má prístup k tomuto nástroju, a po druhé, že prístup nemá nikto iný.

Môže to znieť dosť jednoducho, ale ak sa implementuje bez náležitej starostlivosti, zvyčajne to spôsobí veľkú bezpečnostnú dieru. Ak chcete potrápiť svoju myseľ, zamyslite sa: *Aká je najbežnejšia bezpečnostná diera v správe prístupu spôsobená primitívnou implementáciou?*

Bezpečnostnou chybou je, že systémy zvyčajne nekontrolujú, či sú podmienky na prístup stále platné. Príklad: zamestnanec začína ako Recruiter, ale po pol roku prejde na inú pozíciu. Ak nie je Access Management v spoločnosti správne implementovaný, nespustí sa, keď dôjde k zmene pozície, a zamestnanec môže stále zneužiť svoj prístup k v podstate špehovať kandidátov a získavať osobné informácie.

To je dôvod, prečo vám toľko webových stránok posiela informačné bulletiny roky po tom, čo ste stratili akýkoľvek záujem o akúkoľvek službu, ktorú poskytujú.

Oficiálny názov pre odobratie prístupových práv je **Revocation** (odvolanie, zrušenie) – hovoríme, že práva boli odobraté.

Najväčšou výzvou pri správnej implementácii Access Managementu je nájsť optimálnu rovnováhu medzi dokonalou bezpečnosťou – teda okamžitým zrušením – a dokonalou použiteľnosťou. Aby sme to pochopili, musíme pochopiť, že právo na prístup môže byť teoreticky kedykoľvek odvolané – dokonca aj uprostred toho, keď niekto pristupuje k službe. A keď je právo odobraté, užívateľ by mal okamžite stratiť prístup, čiže inými slovami, systém by ho mal vyhodiť. To však nie je úplne možné vo všetkých scenároch. Internetové stránky sa napríklad prenesú do prehliadača používateľa a kým sa nepokúsi znova načítať stránku alebo prejsť na inú stránku, nie je možné vynútiť overenie ich práv. Ak teda takýto používateľ číta osobné údaje alebo pozerá video, ktoré niekto medzičasom označil ako súkromné, bude k nim mať naďalej prístup.

Úroveň tolerancie zachovania prístupu k informáciám, ku ktorým by už používateľ nemal mať prístup, závisí od citlivosti týchto informácií – prezeranie básne napísanej niekým sa bude považovať za menej citlivé ako prezeranie kódov nukleárneho odpaľovania, len aby sme uviedli extrémne príklady.

Čiastkové procesy

Access management má iba dva podprocesy. Prvým z nich je **Maintenance of Catalogue of User Roles and Access Profiles** (údržba katalógu užívateľských rolí a prístupových profilov). Tento proces pravidelne kontroluje, či dostupné a pridelené práva umožňujú správne používanie našej služby, a tiež bráni používateľom získať alebo zachovať si práva, ktoré by nemali mať. Toto je teda krok, ktorý by mal identifikovať používateľov, ktorí potrebujú upraviť svoje práva, a mal by spustiť ďalší proces.

**Processing of User Access Requests** (spracovanie žiadostí o prístup používateľa) je proces, ktorý reálne vykonáva úpravu práv – preberá  **Requests for Access Rights** (žiadosti o prístupové práva) a podľa požiadavky práva buď pridá, zmení alebo odoberie. Okrem toho tento proces musí mať rozhranie k systémom, pre ktoré spravuje práva, aby tieto systémy mohli kontrolovať, či konkrétny používateľ má skutočne právo k nemu pristupovať.

V Téčku používame naše používateľské účty CIAM na prihlásenie do mnohých nástrojov a systémov. Keď sa pokúsime prihlásiť do ktorejkoľvek z nich, na pozadí sa vykoná dopyt na vzdialenú autentifikáciu a systém, ktorý uchováva prístupové práva, povie príslušnému systému „Áno, používateľ sa môže prihlásiť a jeho práva sú toto a toto“ alebo „Nie , nevpúšťajte používateľa dovnútra“.

Toto použitie CIAM na autentifikáciu je v praxi Access Management.

facilities Management

V Service Operation zostávajú štyri procesy. Bližšie si povieme len o jednom z nich – Facility Management. Ďalšie tri procesy sú mimo rámca ITIL Foundation a budú zhrnuté neskôr.

**Facilities Management** je proces, ktorý riadi skutočné fyzické prostredie, v ktorom sú umiestnené všetky prvky IT infraštruktúry. Cieľom tohto procesu je zabezpečiť optimálne prostredie pre IT infraštruktúru.

Laicky povedané, Facilities management má na starosti všetko chladenie, kúrenie a prúdenie vzduchu, no zároveň zabezpečuje, aby do budov mali prístup len oprávnení pracovníci. Nevyhnutnou súčasťou zodpovednosti za Facilities management je niečo, čo sa nazýva **environmental monitoring** (monitorovanie životného prostredia) – to zahŕňa všetky požiarne senzory, senzory úniku plynu, prípadne seizmické senzory; monitorovala by aj hladinu vody alebo rýchlosť vetra, ak by sa IT infraštruktúra nachádzala na mieste, kde by podzemná voda alebo vietor mohli predstavovať nebezpečenstvo.

Proces **vlastní a spravuje Facilities Manager** – upozorňujeme, že k jednotlivým budovám, ako napríklad ku každému dátovému centru, môžu byť pridelení aj ďalší Facili**ty** Manageri.

Ako si viete predstaviť, Facilities Management dokáže zhromaždiť množstvo informácií z monitorovacích systémov a zo systémov kontroly prístupu a pomocou automatizovaných analytických nástrojov dokáže identifikovať obavy. Tieto obavy môžu byť potom predložené iným procesom alebo sa nimi môže zaoberať samotný Facilities Management.

Facilities Management úzko spolupracuje s procesmi Service and Business Continuity Management. Cieľom tejto spolupráce je mať jasnú stratégiu a podrobné plány na riešenie katastrof, ako je požiar. Z tohto dôvodu je Facilities Management priamo prepojený s predpismi o ochrane zdravia a bezpečnosti (Health and Safety regulations).

Ak si pamätáte kapitolu o Access Managemente, hovorili sme o nájdení najlepšej rovnováhy medzi dokonalou správou prístupu a použiteľnosťou. Kontrola používateľských práv každú sekundu by nebola praktická a vo všeobecnosti akceptujeme, že zrušenie práv môže chvíľu trvať, kým sa dostane do systému, na ktorom používateľ momentálne pracuje.

Facility Management je v podobnom vzťahu k predpisom BOZP. Aby ľudia mohli bezpečne uniknúť počas katastrofy, bezpečnosť (ako security) musí byť trochu ohrozená. Dvere, ktoré musia byť rozbitné v prípade požiaru, nemôžu byť vyrobené z vystuženej ocele, ktorá by zabránila „zlých chlapom“ vstúpiť na miesto a ukradnúť veci.

Jedným zo spôsobov, ako Facilities Management zaisťuje vysokú úroveň bezpečnosti pri súčasnom dodržiavaní bezpečnostných predpisov, je serializácia slabších bezpečnostných prvkov – ako napríklad prinútenie ľudí, aby prešli cez **viacero sklenených dverí** namiesto jedných. Týmto spôsobom, ak sú niektoré z dverí prelomené silou, **zazvoní alarm** a bezpečnostný personál by mal mať dostatok času, aby zabránil krádeži alebo zničeniu infraštruktúry.

Funkcie v Service Operation

Service operation obsahuje aj IT Operations Control, Application Management a Technical Management.

Na rozdiel od všetkých ostatných procesov, ktoré sme spomenuli, tu nejde o skutočné procesy – ITIL ich oficiálne považuje za funkcie. Poďme sa pozrieť na to, čo spravujú.

IT Operations Control

Jednotlivec alebo tím nazývaný **IT Operations Control** je zodpovedný za dohľad nad každodennou prevádzkou IT infraštruktúry. Je to funkcia, ktorá monitoruje a riadi služby IT, aby zabezpečila ich nepretržitú dostupnosť a optimálnu výkonnosť. IT Operations Control zahŕňa činnosti ako monitorovanie systémov, sieťových zariadení a aplikácií, riadenie zálohovania, plánovanie údržby a sledovanie výstrah o stave infraštruktúry. Cieľom je minimalizovať prestoje a zabezpečiť, aby všetky systémy fungovali hladko a v súlade so stanovenými servisnými úrovňami (SLA).Akékoľvek zložitejšie úlohy sa vykonávajú v rámci iných procesov, ako je Change Management.

**Príklad: nemocnica**, ktorá využíva IT Operations Control na riadenie svojej IT infraštruktúry. V nemocnici sú prepojené systémy, ktoré zaznamenávajú vitálne funkcie pacientov v reálnom čase. Ak IT Operations Control zistí zlyhanie monitorovacieho systému (napr. kvôli problému so serverom), tím okamžite koná, aby obnovil spojenie a zaistil, že zdravotnícky personál bude mať nepretržitý prístup k životne dôležitým údajom. Táto funkcia tak priamo prispieva k bezpečnosti pacientov, pretože udržiava nepretržitú dostupnosť kritických systémov.

Application Management

Druhou z týchto funkcií je **Application Management** (správa aplikácií). Je potrebné dávať pozor, aby ste si to **nepomýlili** s Application **Development** (vývojom aplikácií). Application Development vykonáva mnoho činností, aby skonštruoval aplikáciu a potom ju odovzdal do prevádzky; na rozdiel od toho tímy v Application Management zhromažďujú spätnú väzbu a správy o tom, ako aplikácia funguje, môžu školiť ľudí v efektívnejšom používaní tejto aplikácie a odosielať spätnú väzbu vývojárom, ktorí môžu opraviť zistené chyby alebo zlepšiť používateľskú skúsenosť.

Mimoriadne zaujímavé, aj keď stále mimo rámca ITIL Foundation, je skutočnosť, že Application Management má na starosti **Skills Inventory** (inventár zručností). Skills Inventory je katalóg zručností, ktoré sú potrebné na poskytovanie príslušnej IT služby – teraz aj v budúcnosti. Napríklad zručnosť, ktorú potrebujú všetci čašníci a čašníčky, je otváranie fliaš vína, výber pohárov na víno a nalievanie vína. Toto by sa mohlo zaznamenať v inventári zručností ako „zručnosť manipulácie s vínom“. Tímy v Application Management sú zvyčajne prvými ľuďmi, ktorí sa učia novú aplikáciu, a na základe záznamov v inventári zručností navrhnú školiace plány, ktoré tieto zručnosti naučia ostatných zamestnancov.

Oficiálny Owner (vlastník) Application Management je **Application Analyst**, čo je odchýlka od štandardnej terminológie. To zdôrazňuje, že ich zodpovednosťou je **porozumieť aplikáciám** a vysvetľovať ich ostatným používateľom – a nie **vlastniť aplikácie** a rozhodovať o ich funkciách.

Technical Management

A nakoniec tu máme Technical Management. Technical management je vhodné vnímať ako klon Application Managementu, pretože to v podstate aj je z praktického hľadiska. Ak Application Management analyzuje aplikácie a učí ľudí, ako ich používať, potom Technical Management analyzuje technológie a učí ľudí, ako ich ovládať.

Technical Management by teda pripravil školiace plány pre nové technológie – nové typy serverov, routrov, switchov, úložné systémy, káble a periférne zariadenia (hardvérové komponenty, ktoré sa pripájajú k počítaču, aby rozšírili jeho funkcionalitu. Sú to externé zariadenia, ktoré umožňujú vstup a výstup údajov alebo rozšírenie iných funkcií počítača).

Ak ste niekedy videli skutočného IT profesionála postaviť počítač z komponentov alebo pripojiť systém k sieti, možno ste si všimli, že ich pohyb sa javí precíznejší, systematickejší; vedia, kam sa majú dostať a ako dosiahnuť svoj cieľ. Technical management sa snaží o túto úroveň efektívnosti a bezchybnej prevádzky.

Rovnako ako v Application Management, aj tu sa vlastník procesu nazýva **Technical Analyst**, čo opäť zdôrazňuje, že ich cieľom je **porozumieť** technológii a **nie rozhodovať** o tom, ktorá technológia sa použije.

zhrnutie service operation

Pamätajte, že Service Operation sa týka každodennej prevádzky našej služby. Zákazníci a používatelia vznášajú požiadavky **(raising requests)**, ktoré je potrebné splniť **(fulfill)**. Niekedy to vyžaduje udelenie prístupu **(granting access)**, ale musíme to sledovať a odvolať prístup **(revoke access)**, keď už nie je potrebný.

Ak sa niečo pokazí, dúfajme, že nás na to upozorní **Event Management**. Potom je čas otvoriť **incident** a obnoviť normálnu prevádzku **(restore normal operation)**. Ak nevieme ako, alebo ak je výpadok záhadou s neznámou **root cause**, potom ide o **problém** a treba ho preskúmať **(investigate)** a zmeniť na **Known error**, možno s dočasným riešením **(Workaround)**, kým sa nenájde trvalé riešenie **(permanent solution)**.

Trochu v pozadí **Facilities Management** zaisťuje príjemné a stabilné prostredie, zatiaľ čo **Application a Technical Management** podporuje optimálny výkon nášho **hardvéru a softvéru**.