



Překlenutí propasti mezi IT a provozem pro úspěšnou digitální transformaci

Obsah

- | IoT podporuje spolupráci v oblasti IT a operací
- | Nové případy použití a příležitosti
- | Sdílená vize a základní technologie
- | Správný technologický partner



IoT podporuje spolupráci v oblasti IT a operací

Až donedávna mělo obvykle smysl, aby IT a provozní týmy fungovaly jako samostatné jednotky v rámci podniků. Tyto dva světy se navzájem nepřekrývaly. Zatímco se IT týmy zaměřily na nasazení a údržbu síťové infrastruktury společnosti a zvyšování kybernetické bezpečnosti, provozní týmy se zaměřily na každodenní činnosti, jako je správa zařízení, řízení výroby, prodej a marketing a zabezpečení budov.

Vzhledem k tomu, že provozní týmy se při dosahování svých cílů a digitální transformaci podniku stále více spoléhají na řešení IoT, vzniká nová a naléhavá potřeba, aby oba týmy spolupracovaly a sdílely své odborné znalosti. Řešení IoT jsou ideálním způsobem automatizace a urychlení operací za účelem zvýšení agility a kontinuity podnikání i zlepšení zákaznické zkušenosti. Tato řešení však vyžadují připojení stovek nebo tisíců nových zařízení k podnikové síti, což spadá do oblasti IT.

Podniky, které rozbíjejí zdi mezi oddělením IT a provozem a povzbuzují oba týmy k přirozené spolupráci, mohou tato rizika výrazně snížit. Mohou také maximalizovat výhody, které IoT a další iniciativy v oblasti digitální transformace přinášejí do podnikání.

Bílá kniha

Překlenutí propasti mezi IT a provozem pro úspěšnou digitální transformaci



Odpojené týmy zvyšují rizika

IT a provozní týmy, které si navzájem neuvědomují své aktivity nebo které nejsou zkoordinované a nespolupracují, ohrožují iniciativy digitální transformace a společnost z různých hledisek:

- **Kybernetická bezpečnost** Kdy pracovníci IT neví o nových zařízeních IoT implementovaných operačním týmem, nemohou zajistit, aby zařízení vyhovovala firemním bezpečnostním zásadám. Zařízení IoT přicházejí s vysoce variabilními úrovněmi funkcí kybernetické bezpečnosti a nemusí implementovat nejnovější osvědčené postupy ochrany. Tato „stínová IT zařízení“ mohou používat jakýkoli software a mohou být již infikována viry a malwarem. Pokud nejsou kontrolovány, mohou do sítě snadno vnést nové zranitelnosti a vektory útoku.
- **Finanční a provozní efektivita.** Pokud týmy IT a provozu implementují technologická řešení bez vědomí ostatních, může docházet ke zdvojování nákladů a úsilí. Zaměstnanci provozu si například mohou zakoupit řešení pro monitorování a správu zařízení IoT, aniž by věděli, že oddělení IT již má zavedené řešení, které může tyto úkoly provádět. Jediné řešení, které dokáže splnit potřeby IT a provozu, je vždy nákladově nejefektivnější a provozně nejefektivnější varianta.
- **Výkon a spolehlivost.** IT týmy chápou, jak lze firemní síť optimalizovat a doladit tak, aby splňovala specifické požadavky, jako je kvalita služeb (QoS) pro nasazení IoT. Pokud provozní týmy nemohou využít těchto odborných znalostí, existuje větší riziko, že se budou kritické iniciativy digitální transformace realizovat s nedostatky ve výkonu a spolehlivosti, kterým bylo možné předejít.



Nové případy použití a příležitosti

Týmy IT a provozní týmy mají různé oblasti zaměření a odborné znalosti, takže každá skupina přináší jedinečné a důležité schopnosti. Provozní týmy chápou, která řešení IoT mohou společnosti nejlépe pomoci zvýšit efektivitu a snížit náklady. IT organizace pak mají nástroje a know-how pro automatizaci a zjednodušení všech aspektů těchto řešení, od nasazení a monitorování až po údržbu a upgrady — výhody, které se množí s rostoucím rozsahem nasazení Internetu věcí.

Společně mají oba týmy znalosti, dovednosti a nástroje, které společnosti potřebují, aby mohly využít nových případů použití a příležitostí, které zvyšují obchodní úspěch. Zároveň se IT stává klíčovým strategickým zdrojem, který pomáhá operacím i podnikání dosáhnout jeho finančních a provozních cílů.

Když IT a provozní oddělení spolupracují na zavedení bezpečných, nákladově efektivních a spolehlivých řešení Internetu věcí, jsou možnosti neomezené. Následuje jen několik příkladů, které lze snadno přizpůsobit potřebám různých průmyslových odvětví a organizací.

Zvýšení agility a odezvy díky komunikaci v reálném čase

Řešení IoT, která automaticky spojují lidi a systémy založené na událostech v reálném čase, přinášejí do obchodních operací dosud nepoznanou rychlost.

Na letištích mohou být pracovníci odbavující zavazadla upozorněni na to, že letadla brzy přistanou, aby mohli připravit pásové nakladače a přepravní vozidla. Pokud dojde k mimořádné situaci, řešení dokáže automaticky propojit vedení letiště, bezpečnostní týmy a pracovníky donucovacích orgánů, aby mohli koordinovat řešení situace. Ve školách a městech upozornění v reálném čase informují o příjezdu autobusů a pomáhají úředníkům rychle reagovat na neočekávané události.

Snížení nákladů automatizací rutinních úkolů

Mnoho podniků a veřejných zařízení stále spoléhá na časově náročné manuální kontroly při provádění všedních úkolů, jako je kontrola, zda jsou odpadkové koše plné. Díky senzorům, které sledují úroveň odpadu, jsou automaticky upozorněny správné osoby nebo systémy, když každý koš dosáhne předem definované prahové hodnoty. Při ručních kontrolách se neztrácí čas ani peníze, pracovníci údržby mohou trávit více času úkoly s vyšší hodnotou a náklady na pytle na odpady a likvidaci se snižují, protože koše se vyprazdňují pouze v případě potřeby.

Zvýšení efektivity pomocí sledování aktiv

Znalost přesného umístění kritických aktiv za všech okolností pomáhá lidem pracovat efektivněji.

Ve zdravotnických střediscích umožňuje schopnost určit polohu nejbližší dostupné kyslíkové nádrže, vozíku, invalidního vozíku a dalšího vybavení lépe reagovat na potřeby a zefektivnit pracovní postupy. Stejná technologie sledování majetku na letištích umožňuje personálu zjistit, kde se nachází pozemní podpůrné vybavení, jako jsou vlečné vozy, nakladače palet a cateringová vozidla, a zrychlit tak dobu obratu letadla.

Zlepšení zákaznické zkušenosti díky hladkému průběhu cesty

Technologie sledování polohy lze také použít ke zlepšení cesty zákazníka od začátku do konce. Například nemocnice může použít data shromážděná z náramků pro pacienty s podporou IoT k analýze času, který pacienti strávili v jednotlivých fázích péče – včetně pohotovostních oddělení, přijetí, čekárny, radiologie, operačních sálů, zotavení, fyzioterapie a propuštění. Výsledky pak mohou využít k optimalizaci procesů a pracovních postupů za účelem zlepšení zkušeností a spokojenosti pacientů.

Na letištích může vylepšená lokalizační technologie pomoci cestujícím zvolit nejefektivnější trasy přes rozlehlé terminály. S aplikací, která popisuje nejrychlejší cestu z jejich aktuální polohy k východu, je mnohem méně pravděpodobné, že cestující zabloudí nebo se vydají pomalou, spleťitou cestou, která zvyšuje riziko zpoždění letu.

Zvýšení odolnosti monitorováním kritických systémů

Bezpečná a spolehlivá řešení IoT představují ideální způsob, jak mohou poskytovatelé služeb a podniky proaktivně sledovat výkon kritické infrastruktury a systémů, jako jsou distribuční soustavy plynu, vody a elektřiny.

Při těchto typech nasazení senzory automaticky odesílají upozornění při překročení prahových hodnot pro klíčové ukazatele výkonu (KPI), jako je teplota, tlak, vibrace, točivý moment a vlhkost. S okamžitým upozorněním na zhoršení výkonu mohou pracovníci údržby proaktivně řešit problémy, aby zabránili poškození zařízení, poruchám a přerušení servisu.



Zvýšení udržitelnosti pomocí inteligentních řešení budov

Inteligentní řešení budov pomáhají podnikům a vládním organizacím optimalizovat využívání energie a zdrojů tak, aby mohly dosáhnout ekologických cílů a snížit provozní náklady.

Existuje celá řada řešení pro chytré budovy, která se opírají o připojená zařízení Internetu věcí, ale mezi nejběžnější patří řešení, která automatizují systémy osvětlení, vody a vytápění, větrání a klimatizace (HVAC) na základě denní doby, úrovně poptávky a přítomnosti lidí.

Snížení znečištění pomocí inteligentních dopravních řešení

Jelikož města pracují na snižování znečištění ovzduší, stále častěji přijímají řešení IoT, která jim pomáhají sledovat emise vozidel na nejrušnějších silnicích a na křižovatkách, kde dochází k dopravním zácpám. Poté mohou analyzovat shromážděná data a použít výsledné poznatky k cílení vylepšení, která pomáhají zefektivnit toky provozu.

Inteligentní města také využívají technologie IoT k implementaci inteligentních parkovacích řešení, která občanům pomáhají rychleji najít parkovací místa a snížit množství dopravních zácp a emisí vozidel.

Zlepšení shody s předpisy díky úplnému přehledu o všech zařízeních

A konečně, pokud týmy IT a provozu spolupracují na nasazení Internetu věcí a podpůrných síťových technologií, mohou implementovat řešení, jež zajistí přehled a správu všech zařízení přistupujících k síti. Tento úplný přehled usnadňuje prokázání souladu s regulačními normami, podnikovými zásadami a osvědčenými postupy v oblasti kybernetické bezpečnosti. V rámci auditů pak nejsou odhalena žádná znepokojující překvapení. Zařízení se zastaralým firmwarem nebo bezpečnostními záplatami se okamžitě identifikují a riziko vzniku průmyslových pokut se výrazně minimalizuje.

Bílá kniha

Překlenutí propasti mezi IT a provozem pro úspěšnou digitální transformaci





Sdílená vize a základní technologie

Každá organizace je ve svém vývoji a digitální transformaci v jiné fázi, takže neexistuje univerzální přístup ke zvyšování spolupráce mezi IT a provozními týmy. Zatímco některé organizace jsou na své cestě digitalizace dále než jiné, většina z nich stále používá kombinaci moderních a starších technologií, které odrážejí jejich jedinečnou historii.

Bez ohledu na to, kde se dnes podnik nachází, existují běžná témata a technologické aspekty pro IT a provozní týmy, které chtějí spolupracovat. Diskuse by měly začít u požadavků na vytváření sítí a kybernetickou bezpečnost pro navrhovaná řešení IoT, například:

- Typy zařízení, která budou mít přístup k síti, a médium připojení, které budou vyžadovat, například kabelové nebo bezdrátové, vnitřní nebo venkovní. Dále je třeba vzít v úvahu faktory prostředí, jako je extrémní teplo, chlad, vibrace, vítr, déšť, sníh nebo led.
- Zásady kybernetické bezpečnosti, které by měl každý typ zařízení dodržovat, a aplikace, se kterými může každý typ zařízení komunikovat
- Jak by se měly informace z jednotlivých typů zařízení propojit s informacemi ze sítě a podnikových systémů, aby se zajistilo, že se správné poznatky a data dostanou ke správným lidem ve správný čas.

Jakmile je definována sdílená vize řešení IoT, je čas vyhodnotit technologie potřebné k úspěšné implementaci vize.

Pro mnoho týmů IT se nové požadavky na podporu vysokých nároků na připojení k Internetu věcí z různých oddělení mohou zdát zdrcující. Přední dnes dostupná síťová řešení však byla navržena tak, aby bezpečně podporovala a zjednodušovala všechny aspekty i těch největších nasazení IoT. Se správným přístupem k síťové infrastruktuře a platformám pro správu se IT týmy mohou plynule vyvinout z potenciální překážky v nasazení Internetu věcí na klíčový podnikatelský potenciál.



Bezpečné automatizované sítě zjednodušují nasazení IoT

Moderní sítě automaticky detekují nová zařízení IoT a mohou klasifikovat a segmentovat každý typ zařízení na základě zásad kybernetické bezpečnosti. Podporují také síťovou architekturu s nulovou důvěrou (ZTNA), která vytváří „předpoklad nikomu nedůvěřovat“ pro každého uživatele, zařízení nebo aplikaci bez ohledu na to, kde se nachází (na pracovišti, v cloudu nebo mimo pracoviště), aby se minimalizovala rizika kybernetické bezpečnosti. Nejpokročilejší síťová řešení podporují makro- i mikrosegmentaci a umožňují podrobný přístup ke kybernetické bezpečnosti:

- Makrosegmentace odděluje uživatele, zařízení a aplikace v síti podle jejich funkční domény. Například stolní a IP telefonie jsou jedním makrosegmentem, zatímco video dohled je jiný makrosegment.
- Mikrosegmentace definuje, jak mohou uživatelé, zařízení a aplikace v makrosegmentu vzájemně interagovat, a obvykle se řídí velmi specifickými bezpečnostními zásadami.

V nemocnici by mohl být makrosegment věnován zdravotnickému vybavení, jako jsou monitory pacientů, a konkrétní skupině uživatelů. Makrosegment lze také použít k zajištění přístupu k síti se specifickými parametry kvality služeb (QoS) a bezpečnostními parametry. Senzory a ovládací prvky pro osvětlení a systémy HVAC by byly zařazeny do samostatného makrosegmentu, stejně jako technologie související s bezpečností, jako jsou kamery CCTV a systémy zamykání dveří. Při tomto typu segmentace by kompromitovaný termostat nebyl schopen komunikovat s monitorem pacienta nebo systémem zámku dveří.

Mikrosegmentace reguluje aktivity v rámci makrosegmentu. Například bezpečnostní kamera by neměla mít možnost propojení se zámek dveří, přestože se nacházejí ve stejném makrosegmentu souvisejícím s bezpečností.

Jednotná správa sítě zvyšuje efektivitu a konzistenci

Použití jediné platformy pro správu a analýzu, která poskytuje ucelený pohled na všechny kabelové a bezdrátové sítě a zařízení Internetu věcí, umožňuje rychlejší, jednodušší a méně rizikovou správu a řešení problémů ve srovnání s používáním několika různých systémů správy. Pokud má například zařízení Internetu věcí problémy s připojením, může provozovatel sítě určit, zda je hlavní příčinou problému samotné zařízení nebo zařízení kabelové či bezdrátové sítě, ke které se připojuje.

Podnik se také může vyhnout dodatečným nákladům spojeným s nákupem a provozem více systémů správy kabelových, bezdrátových a IoT zařízení. A zásady kybernetické bezpečnosti jsou uplatňovány konzistentně napříč všemi typy zařízení, což snižuje riziko zavedení zranitelností zabezpečení do sítě.



Nové inovace spojují lidi a informace

IT a provozní týmy by měly také vyhodnotit nové technologie, které jim pomohou co nejlépe využívat data ze zařízení IoT.

Dobrým příkladem nedávného pokroku, který by měl být vzat v úvahu, jsou aplikace pro sledování majetku, které identifikují polohu majetku a osob v reálném čase. Tyto aplikace používají tagy s podporou GPS, BLE nebo RFID k rychlému a snadnému sledování a hledání aktiv nebo lidí. Zahrnují také analýzy, které pomáhají podnikům optimalizovat využití jejich aktiv, například:

- Jak dlouho lidé museli čekat na přístup k vybavení
- Která oddělení nejčastěji používají jednotlivé typy zařízení
- Které zařízení se používá nejméně
- Jak často se zařízení pohybuje v areálu a jak daleko každý den cestuje
- Kdy naposledy proběhl servis vybavení

Dalším dobrým příkladem jsou motory pracovního postupu. Tyto platformy kombinují data ze zařízení IoT, síťové infrastruktury, podnikových aplikací a dalších systémů a sdělují je lidem, když to nejvíce potřebují. Pokud například senzor IoT hlásí únik oxidu uhelnatého ve veřejné budově, modul pracovního postupu může okamžitě a současně upozornit interní týmy údržby, externí odborníky, týmy pro správu budov a zabezpečení budov. Může také umožnit, aby se všechny informované strany spontánně připojily k chatu, hlasové nebo video konferenci a diskutovaly o problému. Každá strana těží z informací v reálném čase pocházejících ze senzorů IoT a může současně vidět video monitorovací kanál, který jim pomáhá lépe posoudit situaci.



Ten správný technologický partner

Vzhledem k tomu, že IT a provozní týmy chtějí zvýšit spolupráci, budou potřebovat zkušeného technologického partnera, který bude poskytovat poradenství, odborné znalosti a řešení po celou dobu jejich cesty.

Alcatel-Lucent Enterprise oceňuje finanční a provozní výhody, které podniky získají, když IT a provozní týmy spolupracují na iniciativách digitální transformace. Chápeme také, jak mohou IT a provozní týmy využívat moderní technologie a řešení ke zvýšení kybernetické bezpečnosti, spolehlivosti a efektivity při současném snížení rizik a nákladů. Naše řešení zjednodušují a urychlují digitální transformaci bez ohledu na to, v jaké fázi vývoje se dnes organizace nacházejí:

- Kabelová a bezdrátová síťová řešení s integrovaným automatizovaným připojením IoT zjednodušují nasazení a poskytují plnou podporu bezpečnostních strategií ZTNA
- Jednotná řešení pro správu sítě poskytují soudržnou správu a celosíťový přehled o všech kabelových a bezdrátových zařízeních, která k síti přistupují.
- Řešení pro sledování majetku využívají technologii BLE pro vysoce přesné a zároveň energeticky úsporné sledování polohy.
- Pracovní postup a cloudová komunikační platforma [Rainbow™ od společnosti Alcatel-Lucent Enterprise](#) propojuje lidi, stroje a procesy pomocí chatu, hlasu a videa

Naše řešení podporujeme odbornými službami, které pomáhají našim zákazníkům realizovat jejich cíle digitální transformace efektivním a nákladově efektivním způsobem.

Bílá kniha

Překlenutí propasti mezi IT a provozem pro úspěšnou digitální transformaci

Podpora cílů digitální transformace zákazníků

Díky naší jedinečné kombinaci technologických řešení a odborných znalostí s námi spolupracují přední organizace z celého světa a různých odvětví, například:

- [Liverpool City Region Combined Authority](#) ve Velké Británii, která využívá síťová, řídicí a komunikační řešení ALE ke zlepšení komfortu cestujících a efektivity provozu. Naše řešení podporují kritická zařízení Internetu věcí pro systémy CCTV, řízení dopravy, detekci požáru a kouře a systémy dohledu a sběru dat (SCADA), stejně jako služby mýtného, jako jsou automatické rozpoznávání registračních značek (ANPR) a integrace interkomových systémů. Organizace také podporuje plánovaná vylepšení, jako jsou komunikace mezi loděmi na břeh, konektivita pro říční trajekty a inteligentní rozšíření jízdenek pro veřejnou dopravu.
- [Metropolitní správa Bangkoku](#) v Thajsku využívá síťová a řídicí řešení společnosti ALE k vytvoření vysokorychlostní redundantní sítě pro chytrá městská zařízení Internetu věcí, která pomohou zlepšit kvalitu života občanů a ekonomické příležitosti. Bangkok jako hlavní město Thajska hraje díky své moderní síti a inovacím v oblasti chytrých měst klíčovou roli při plnění cílů Thajska 4.0.
- [Společnost Aster DM Healthcare](#) ve Spojených arabských emirátech (SAE) využívá síťová řešení, řešení pro správu, komunikaci a spolupráci od společnosti ALE, aby poskytla personálu nemocnice nepřetržitý přístup ke zdravotnickým datům a kritickým zdravotnickým aplikacím – kdykoli a kdekoli je potřeba. Konvergované řešení také umožňuje zaměstnancům společnosti Aster se hladce a bezpečně spojit a spolupracovat napříč weby, i když jsou na cestách, takže mohou trávit více času s pacienty. A poskytuje pacientům spolehlivý přístup k Wi-Fi, aby mohli zůstat ve spojení s rodinou a přáteli v zařízeních Aster.
- [Kalifornská státní univerzita](#) v USA používá síťová řešení ALE ke zlepšení zabezpečení, zajištění všudypřítomné Wi-Fi a poskytování otevřených sdílených cloudových služeb, které zlepšují celkový dojem z kampusu. Vysoce spolehlivá a flexibilní síť bezpečně podporuje více než 500 000 uživatelů ve více než 20 univerzitních kampusech a pomohla ušetřit více než 100 milionů USD na nákladech na infrastrukturu.
- [Společnost Energy One](#) v Austrálii používá řešení ALE pro správu a řízení sítí k automatizaci a zjednodušení správy a údržby sítí ve svých pobočkách v Sydney a Melbourne. Autonomní síť usnadňuje zavádění nových pracovišť, uvolňuje pracovníky IT, aby se mohli soustředit na prioritní úkoly, a zlepšuje výkon sítě a pokrytí Wi-Fi, takže zaměstnanci mohou pracovat produktivněji díky větší mobilitě a konzistentnímu uživatelskému prostředí na různých místech.



Další informace

Pokud se chcete dozvědět, jak můžeme vaší organizaci pomoci s efektivní a nákladově efektivní digitální transformací, [podívejte se na naše webové stránky](#) nebo nás ještě dnes [kontaktujte](#) a proberte s námi vaše konkrétní potřeby.

