



Pokyny IT pro navrhování IP video systému

Devět kritických IT problémů při navrhování IP video systému



Obsah

Úvod.....	3
1. Úloha IT odbornosti ve video systémech	4
2. Určení správné velikosti zařízení pro splnění potřeb video dohledu	5
3. Klíčová úloha práce v síti	6
4. Zdůraznění významu hodnoty nad významem ceny	7
5. Kybernetické bezpečnostní hrozby a nápravy	7
6. Limity přístupu „fyzicky izolováno“	8
7. Zamezení jakékoli ztráty video dat	9
8. Řízení životních cyklů v IP systémech dohledu	10
9. Ekosystém IT ve video systémech	10

Společnost Alcatel-Lucent Enterprise pověřila SourceSecurity.com vytvořením tohoto dokumentu.



Úvod

Systém video dohledu má specializované potřeby, pokud jde o informační technologie (IT). Zatímco digitální video systém může používat stejné technologie jako jiné IT systémy, jsou systémy video dohledu konfigurovány odlišně a s ohledem na své specifické potřeby.

Video je náročnější prostředí a zvyšuje pracovní zátěž pro každou část IT systému. Vzhledem ke stresu, a zejména v případě většího podnikového systému, věci mohou začít selhávat. Výběr správného zařízení pro danou práci zajišťuje větší spolehlivost v průběhu času.

Společnost Alcatel-Lucent Enterprise spolupracovala s odborníky z oboru a to ze SourceSecurity.com a Stone Security na identifikaci devíti kritických IT problémů při navrhování IP video systému. V tomto metodickém dokumentu zkoumáme, jak specializované potřeby systému video dohledu ovlivňují to, jaké IT technologie jsou zaváděny a jak jsou využívány.



1. Úloha IT odbornosti ve video systémech

Navrhování a vytvoření systému video dohledu založeného na internetovém protokolu (IP) vyžaduje vysokou úroveň IT odbornosti v komunitě integrátorů.

Někteří integrátoři mají dostatečné dovednosti pro odborné spuštění IP video systému, zatímco jiní mohou mít potíže.

Zvláštní školení a certifikace, které jsou běžné pro většinu světa IT, mohou integrátorům umožnit poskytovat požadovanou vysokou úroveň služeb. Chcete-li začít, instalační pracovníci musí mít správné schopnosti a základní pochopení práce v síti a dovednosti při odstraňování problémů.

Integrátoři mohou zajistit znalou pracovní sílu tím, že omezí škálu volby technologií a zajistí, že každý zaměstnanec je dobře vyškolen v menším počtu technologií. Výběr nejlepších řešení v dané třídě a zajištění toho, aby zaměstnanci byli odborníky na tyto produkty, jsou faktory umožňující integrátorovi dodávat zákazníkům systém vyšší kvality.

Omezení produktového mixu také umožňuje integrátorovi lépe porozumět šíři funkcí nabízených kterýmkoli daným produktem. Příliš často si zákazník kupuje systém, který nabízí celou řadu funkcí, a poté používá pouze omezený počet těchto funkcí v každodenním provozu, čímž oslabuje hodnotu systému, za který zaplatil.

Integrátoři mohou zákazníkům pomoci tím, že je vzdělávají, aby z jakéhokoli systému, který si koupí, uvolnili plnou hodnotu.

Integrátoři se mohou také spolehnout na předkonzultační služby výrobců zařízení, které integrátory vedou. V některých případech mají výrobci zařízení specifické znalosti o různých vertikálních trzích, které se nahromadily během historie služeb pro tyto trhy.

Výrobci, kteří to s určitým vertikálním trhem myslí vážně, budou zaměstnávat odborníky z oboru, aby zajistili podporu, která je specifická pro potřeby každého zákazníka. Jejich pokyny mohou integrátorům pomoci uspět na nových trzích a/nebo zefektivnit nejlepší postupy pro trhy, na kterých působí.

Výrobci také poskytují školení a certifikace, aby zajistili, že integrátoři jsou dobře vybaveni k instalaci svých systémů. Efektivní a věcné školení by mělo být prezentováno v kratších lekcích, které respektují hodnotu času každého účastníka.

2. Určení správné velikosti zařízení pro splnění potřeb video dohledu

Problémy, jako je šířka pásma a požadavky na napájení přes Ethernet (PoE), jsou ve video systému důležitými proměnnými. A video server má vyšší zatížení, zejména pokud jde o video z živého zdroje. Každý bit dat přistane na serveru, dokonce i data, která nejsou zaznamenávána.

Video je chráněno dočasným uchováváním ve vyrovnávací paměti, což zajišťuje, že existuje alespoň několik sekund videa, které lze zachovat před faktickým video záznamem spouštějícím alarm. V případě identifikace obrazu přicházejícího z větší vzdálenosti mohou být potřebné delší období uchovávání. Všechny vstupy a výstupy procházejí serverem, i když omezené množství dat bude zapsáno do dlouhodobého úložiště.

Existuje zásadní rozdíl mezi tím, jak integrátoři bezpečnostních systémů vnímají velikost systému, a tím, jak to vidí IT profesionálové. Systémoví integrátoři s větší pravděpodobností mluví z hlediska počtu kamer, zatímco IT profesionálové s větší pravděpodobností hovoří o správě dat ze systému. Tyto dvě věci jsou samozřejmě vnitřně propojené, ale vztah není lineární. Obecně platí, že vyšší počet kamer odpovídá většímu množství dat, které má IT oddělení spravovat. Existují však i další faktory, které ovlivňují potřeby dat, jako je počet snímků, požadavky na kvalitu obrazu, potřeby úložiště, aplikace den/noc a použití analýzy videa.

Klíčovou dovedností při specifikaci IP bezpečnostního systému je převést požadavky na vybavení a funkčnost systému na údaje nezbytné pro splnění těchto potřeb. U místního systému se to rovná potřebě určit počítačový server, který maximalizuje výkon systému a zároveň snižuje náklady. Problémy, jako virtualizace a cloudové systémy, mohou komplikovat tuto rovnici a poskytnout novou flexibilitu.

Další proměnnou související s návrhem systému je použití kamer na okraji sítě k nahrávání videa pomocí SD karet. Dnes existují dokonce systémy, které jsou „bez serveru“; například veškeré nahrávání probíhá na okraji sítě. Takový přístup ve skutečnosti odvádí výpočetní zátěž ze serveru na okraj sítě, což vede ke snížení potřeby kapacity serveru. Dnešní kamery poskytují data nad rámec video streamu, jako jsou metadata a zvuk, což také ovlivňuje design systému.

IT profesionálové by měli mít důkladný přehled o celkovém systému, jako informace co bude připojeno, snímkové frekvence, rozlišení a video kodeky kamer. S těmito informacemi mohou vypočítat požadavky ohledně sítě, napájení, serverů, kapacity disku, paměti, úložiště a to, zda používat cloudové nebo místní systémy. To zajišťuje důkladný a promyšlený přístup k návrhu a nasazení.

Výrobci poskytují softwarové „kalkulačky“, které pomáhají integrátorům navrhovat systémy převedením systémových požadavků do specifikací konkrétních zařízení. Mějte na paměti, že výpočty by měly splňovat nebo překonávat očekávání a umožňovat budoucí růst.

Implementace cloudových systémů je další proměnnou, pokud jde o návrh systémů video dohledu. Tato jasná tendence směřuje k využívání více cloudových systémů pro video dohled. Výběr cloudových řešení nebo řešení v místě by však měl být proveden případ od případu. Návrháři systémů a koncoví uživatelé by měli odolat zdánlivé nevyhnutelnosti cloudu a raději se rozhodovat na základě potřeb zákazníka.

Mnoho výrobců je pod tlakem, aby přesunuli své systémy do cloudu, ale v ideálním případě by měli svým zákazníkům poskytnout výběr systémů a ne univerzální řešení.

Výrobci jsou v dobré pozici, aby poradili zákazníkům ohledně vhodnosti cloudové konfigurace oproti návrhu řešení v místě. Integrátoři by také měli být dobře obeznámeni s výhodami každého z přístupů nebo usnadnit zákazníkovi rozhodnutí pro jeden z nich. Trh by neměl tlačit aplikace do cloudu, pokud to není optimální přístup pro každého jednotlivého zákazníka.

3. Klíčová role práce v síti

Video systém je jen tak silný jako jeho nejslabší článek. Síťové přepínače nemusí být tak viditelné jako kamery a VMS (virtuálně řízené servery), ale nejsou o nic méně kritické.

Stává se však, že zákazníci považují provoz sítě za samozřejmost a věnují malou pozornost tomu, jak funguje nebo jak maximalizovat její užitečnost. Ve skutečnosti někteří zákazníci chtějí nainstalovat video systém s užitím stávající síťové infrastruktury. To je možné, ale schopnost optimalizovat síťovou část videosystému může být omezena.

V ideálním případě se zákazník rozhodne pro nejlepší přepínače pro video dohled, což zajistí systém, který bude fungovat spolehlivě a efektivně.

Každý videosystém je odlišný, takže věnování zvláštní pozornosti jeho individualizovaným požadavkům zajišťuje, že systém splní svou unikátní misi. Když uvádíme do provozu systém, síť by neměla být považována za dodatečný nápad. Spíše by vše mělo být pečlivě sestaveno s užitím nejlepších součástí, aby byl umožněn a zlepšen provoz v celé šíři systému.

Přepínače, které pracují rychlostí „wire speed“ (přenos dat bez účasti nadřazeného softwaru, tedy maximální rychlostí kterou dovoluje hardware), což znamená, že mají dostatečný výpočetní výkon pro zvládnutí plné rychlosti Ethernetu při minimálních velikostech paketů, jsou nyní v tomto odvětví standardem. Novým bodem rozlišování mezi přepínači je schopnost porozumět jejich provozu a řídit jej.

Neřízené přepínače jsou na trhu dostupné, ale nepoužívají se typicky pro komerční a/nebo podnikové aplikace. Jsou určeny pro použití v malých sítích se základními potřebami; není třeba konfigurovat žádné nastavení.

Naopak řízené přepínače umožňují detekci a diagnostiku problémů s výkonem a zajišťují spolehlivý výkon systémů video dohledu. Umožňují uživatelům zhruba vidět, co by mohlo působit problémy v systému a poskytují pochopení toho, jak tyto informace vypadají.

Hodnota řízených přepínačů, které jsou plně konfigurovatelné, přizpůsobitelné a poskytují škálu dat o výkonu, bude zřejmě v průběhu životnosti systému, protože poskytují důležité náhledy do provozu systému a umožňují snadnější odstranění potíží při identifikaci problémů.

Přepínače by měly být navrženy tak, aby se vypořádaly s potřebami IP video systémů. Například v případě přepínače se 16 porty, je k dispozici dostatečné užití a spotřeba energie pro provoz všech videokamer připojených k přepínači. Dnešní PoE kamery čerpají více energie než předchozí generace. Integrátoři potřebují vědět, že přepínač poskytuje dostatečnou energii pro zvládnutí počtu kamer a pro budoucí růst.

„Když provádíme výběr hardwaru, chceme, aby každý přepínač měl způsobilost pro šířku pásma, kalkulované užití a spotřebu energie a byl řízeným přepínačem, který nám ušetří obrovské množství času při řešení problémů. Šetří nám peníze a šetří peníze zákazníků. Je to více investic na začátku, ale v dlouhodobém horizontu se to vyplatí vytvořením funkčnějšího systému.“

Aaron H. Simpson, prezident a technický ředitel, Stone Security

4. Zdůraznění významu hodnoty nad významem ceny

Spolehlivost je pro video dohled rozhodující a začíná výběrem zařízení.

Specifikace méně kvalitních součástí se v danou chvíli může zdát jako ekonomická nutnost. V dlouhodobém horizontu však bude provoz systému trpět. Náklady volby provozu nikoli optimálního nemusí být při navrhování systému zřejmé, ale postupem času se projeví zcela jasně.

Na druhou stranu, výběr lepšího vybavení - i když je dražší - se vyplatí.

Je rozhodující zvážit náklady (například cenu lepšího vybavení) oproti rizikům nedostatečnosti systému nebo selhání. Při hodnocení nákladů a rizik je nejlepší strategií použít přístup celkových nákladů vlastnictví (TCO). Dalším dlouhodobým nákladovým prvkem, který je třeba zvážit, je hodnota otevřených systémů, které mohou zajistit flexibilitu při rozšiřování nebo změně systému v budoucnu.

Vždy je nejlepší spolupracovat s dodavatelem, který nabízí produkt, kterému důvěřuje a který může dlouhodobě podporovat.

5. Kybernetické bezpečnostní hrozby a nápravy

Historicky byla v odvětví fyzické bezpečnosti ironií nedostatečná pozornost věnovaná kybernetické bezpečnosti IP systémů.

Naštěstí investoři v oblasti fyzické bezpečnosti nyní věnují větší pozornost obavám o kybernetickou bezpečnost na všech úrovních a v celém dodavatelském řetězci fyzické bezpečnosti. Ve skutečnosti se kybernetická bezpečnost stala jedním z klíčových pilířů rozhodovacího procesu pro větší bezpečnostní video systémy.

Minimálním krokem směrem k ochraně před kybernetickými hrozbami a k omezení přístupu do systému je vyhnout se používání výchozích hesel. Ta jsou méně bezpečné a hacker nebo bot je snadněji uhodne. Ve skutečnosti, byla výchozí hesla v Kalifornii zakázána.

Rizika kybernetické bezpečnosti začínají v dodavatelském řetězci, kde útoky mohou ohrozit produkt ještě předtím, než je dodán. Analýza produktu na možné útoky typu „backdoor“ (zadní vrátka) nebo „buffer overflow“ (přetečení vyrovnávací paměti) před dodáním může zmírnit hrozbu. Zákazníci se také mohou rozhodnout virtuálně nainstalovat „good code“ (dobrý = snadno čitelný, srozumitelný kód) po dodání hardwarových produktů, čímž zajistí kybernetickou bezpečnost a přepsání jakéhokoli škodlivého kódu, který mohl být nainstalován během přepravy.

Existuje také řada opatření v oblasti kybernetické bezpečnosti, kterými je třeba se zabývat během instalace a v různých fázích implementace systému. Například „learned port security“ (přiřazená bezpečnost portu) zajišťuje, že k portu přistupuje pouze oprávněné zařízení. Pokud se neoprávněné zařízení pokusí připojit k systému - například připojit novou kameru - spustí se výstraha a přístup k portu je odepřen, dokud nebude schválen člověkem.

Technologie Shortest Path Bridging (SPB) (přemostění nejkratší cestou) může zabránit přeskokování škodlivých aktivit z jednoho systému do druhého. Pravidla jsou nastavena tak, aby kamera mohla streamovat pouze do rekordéru a v sítích s více položkami IoT (internetu věcí) je nasazena další výkonná segmentující technologie.

Systémy by měly zakázat nezabezpečené protokoly, jako jsou FTP a Telnet, které usnadňují komunikaci v síti, ale mohou hackerům poskytnout další příležitosti. Tyto funkce by měly být „ve výchozím nastavení zabezpečené“, aby neumožňovaly připojení k síti, pokud to není úmyslné.

Efektivní kybernetická bezpečnost také vyžaduje omezení fyzického přístupu k systému. Pokud je přepínač nasazen ve skříni správce, kde je fyzický přístup otevřen všem, pak není dobře chráněn. Povolení fyzického přístupu k systému usnadňuje komukoli - včetně zaměstnance představujícího vnitřní hrozbu - připojit notebook a získat přístup k celému systému.

Kamery by jako přístup „hloubkové obrany“ měly zaznamenávat přistoupení k síťovým zařízením.



6. Limity přístupu „fyzicky izolováno“

Kdy jde o ochranu video systémů před kybernetickými útoky prostřednictvím internetu, historicky bylo běžným přístupem vytvoření fyzicky izolovaných systémů.

Fyzicky izolovaný systém zahrnuje izolaci počítače nebo sítě a zabránění navázání externího připojení. Protože fyzicky izolovaný počítač je fyzicky oddělený a neschopný bezdrátově nebo fyzicky se připojit k jiným počítačům nebo síťovým zařízením, je tento přístup považován za všelék k zajištění kybernetické bezpečnosti videosystému.

Ale spoléhat se na fyzickou izolaci jako na jedinou ochranu kybernetické bezpečnosti je riskantní návrh. Existuje celá řada situací, kdy může být fyzicky izolovaný systém vystaven internetu, třeba jen na krátkou dobu. Když k tomu dojde, systém závisí na jakýchkoli dalších opatřeních kybernetické bezpečnosti - pokud existují - aby jej ochránila před katastrofou.

Předpoklad, že systém bude navždy fyzicky izolován, není řešením pro kybernetickou bezpečnost. Místo toho je katastrofou jen čekající na uskutečnění.

Systémy fyzicky izolované také nejsou schopny využívat výhod umělé inteligence (AI) a dalších funkcí, které závisí na přístupu k mnoha uživatelům a analýze sdílených zkušeností. Data od jednoho zákazníka nejsou tak užitečná jako data od stovek zákazníků, která jsou k dispozici v cloudu. Systémy fyzicky izolované neumožňují zákazníkům využívat další hodnotu chytrější analytiky. Vzdát se některých dat (což se stává s ohledem na soukromí) je cena, kterou zákazníci platí za využití větší hodnoty.

Vzhledem k dnešním požadavkům zákazníků na připojení a nepřetržitý přístup ke svým systémům je použití systémů fyzicky izolovaných stále omezenější.

Organizace mají také tendenci odmítat vyhlídku na vytvoření zcela oddělené síťové infrastruktury pro video dohled. Neexistuje nic jako „oddělená, bezpečná“ síť.

7. Zamezení jakékoli ztráty video dat

Ztracená data jsou problémem pro jakýkoli IT systém, ale mnohem více pro IT systémy, které poskytují video dohled. Systém video dohledu je kritický úkol a musí fungovat 24/7. Neexistují žádné prostoje, které by administrátorům umožnily diagnostikovat a řešit jakékoli problémy se ztrátou dat; spíše je nutné zabývat se problémy trvale a v reálném čase.

Zde mohou pomoci řízené přepínače. Řízené přepínače umožňují správcům systému rychle diagnostikovat jakýkoli problém se ztrátou dat a zabývat se jím. Mohou také snadno identifikovat zdroj(e) ztráty dat. Neexistuje žádná možnost „ukázat prstem“, pokud jde o to, která systémová součást je v poruše.

Pakety mohou být ztraceny kvůli převedení přenosu dat z optických vláken na měď a Ethernet. Elektrické přenašeče se používají k přeložení dat z přenosu vlákny na elektrický přenos a zařízení mohou být zdrojem ztracených datových paketů.

Ve video dohledu se ztracený paket dat rovná ohrožení obrazu videa - což způsobí, že je ve skutečnosti navždy ztracen. Neexistuje žádný způsob, jak obnovit obrazy videa, které jsou ztraceny během výpadků při prostoji. Zvažte například aplikaci pro kasino, kde následkem selhání videosystému je ztráta pokrytí herního stolu, což zase může znamenat i ztrátu příjmů.

V široké škále aplikací pro video dohled je nutná redundance, aby byl zajištěn nepřetržitý provoz 24/7.

Potřeba spolehlivosti musí být zvážena v kontextu riziko oproti přínosu. Systém může být levnější, méně složitý a/nebo méně tolerantní vůči chybám, ale takový systém nemusí fungovat tak, jak bylo zamýšleno - což má své vlastní náklady.

Další proměnná, která může způsobit problémy s výkonem ve video systémech, se točí kolem rozdílu mezi unicastem (přenosem dat jednomu příjemci) a multicastem (přenosem dat více příjemcům), což jsou dvě metody odesílání dat po síti. Unicast poskytuje komunikační model typu jeden jednomu (one-to-one), ve kterém jeden odesílatel doručuje data jednomu příjemci. Naproti tomu multicast je model typu jeden mnohým (one-to-many), ve kterém jeden odesílatel doručuje data několika příjemcům.

Mnoho aplikací video dohledu pracuje v režimu unicast. To znamená, že kamera je monitorována v reálném čase jednotlivcem - jedná se o jeden video stream.

Některé aplikace však vyžadují multicast, ve kterém je jeden video stream prohlížen více uživateli. Problémy vznikají při přechodu systému z typu unicast na multicast. Přechod zahrnuje více než jen „přepnutí přepínače“ a nuance a podrobnosti přechodu mohou způsobit problémy s výkonem systému. Problémy nastanou, pokud jsou části systému nastaveny pro typ unicast, když by měly být typu multicast nebo naopak. Správná konfigurace tohoto bodu v celém systému je zásadní.

Funkce inteligentního síťového poradce umožňují koncovému uživateli pochopit, co je normální z hlediska výkonu sítě, a pak rozpoznat, když je něco neobvyklé nebo mimo hranice obvyklých očekávání. Jakékoli odchylky jsou hlášeny automaticky a lidé mohou podle potřeby zasáhnout a na problémy se zaměřit.



8. Řízení životních cyklů v IP systémech dohledu

Ve světě IT mohou životní cykly produktů trvat tři až 10 let v závislosti na odvětví a produktu. Existují protokoly pro zaměření se na problémy, jako doba mezi poruchami (MTBF), firmware a bezpečnostní záplaty.

Na scéně video dohledu byly životní cykly produktů historicky delší - v terénu stále fungují desítky let staré videokamery. Přizpůsobení strategií správy IT pro IP video systémy může odhalit odpojení.

Podpora IT poskytovaná výrobcem poskytuje integrátorovi a koncovému uživateli obrovskou hodnotu. Historicky delší životní cykly v oblasti fyzického zabezpečení vedly k tomu, že systémy pokračují v provozu i po očekávaném období a v nepodporovaném prostředí.

Pokračování v používání zařízení, které výrobce nepodporuje, má neodmyslitelná rizika. Například selhání aktualizace firmwaru může otevřít dveře kybernetickým hrozbám.

Většina zařízení má dnes pětiletou záruku a realisticky by zařízení mohla pokračovat v provozu dalších pět let. S rychle se měnícím technologickým prostředím však většina zákazníků bude chtít využít nejaktuálnějších schopností. Technologická akcelerace se ve skutečnosti rovná kratším životním cyklům v oblasti zabezpečení, stejně jako takto působí v širším prostředí IT a práce v síti.

9. Ekosystém IT ve video systémech

Jednotný ekosystém IT je nejlepším přístupem k zajištění úspěšného IP video systému. Úspěch každé nové technologie závisí na ekosystému IT, který ji podporuje. Záležitosti jako je interoperabilita hardwaru a softwaru, zajišťují hladký provoz systému.

Otevřené standardy zajišťují maximální flexibilitu pro zákazníky v současnosti i v budoucnosti. Užitečné jsou také zjednodušené nabídky. Například [Alcatel-Lucent Enterprise](#) má jediný operační systém, který funguje s každým ethernetovým přepínačem, který společnost prodává.

Abyste zajistili úspěch, udržujte strategii zahrnující produkty, které „hrají dobře“ ve svém prostředí a s dalšími produkty v ekosystému.

Úspěšný ekosystém IT nenastane jen tak. Spíše je živěn partnery v oboru, kteří spolupracují, aby zajistili úspěch. Zásady, jako je otevřenost a interoperabilita, přispívají k ekosystému IT. Úspěch zvyšuje výkon každé součásti systému a systému jako celku.

Zjistěte víc o řešeních video dohledu Alcatel-Lucent Enterprise.