



Upřednostnění odolnosti a bezpečnosti jako priorit

Řešení pro vládu od Alcatel-Lucent Enterprise

Obsah

- | Přehled
- | Proč je spolupráce IT/OT kritická
- | Odolná a bezpečná síťová řešení
- | Odolná a bezpečná komunikační řešení
- | Ochrana lidí a aktiv
- | Nezávislost a bezpečnost dat



Přehled

Vzhledem k rostoucím globálním výzvám a zvýšeným kybernetickým a fyzickým rizikům musí vlády upřednostňovat řízení rizik, chránit kritickou infrastrukturu a chránit občany. Podle společnosti CloudSek počet kybernetických útoků proti vládě vzrostl v roce 2022 o 95 %.¹ Předpokládá se, že provoz vlády pokračuje bez ohledu na situaci a že občané budou udržováni v bezpečí. V dnešním globálním klimatu je důležitější než kdy jindy udržovat bezpečnost dat, chránit nezávislost dat a zajistit dostupnost služeb.

Veřejný sektor a proč jsou ICT (informační a komunikační technologie) důležitější než kdy jindy

Digitální transformace ve veřejném sektoru v posledních letech rychle pokročila a stále více občanů má přístup k digitálním službám. Digitální

transformace také umožnila vládním zaměstnancům přijmout pracovní styl práce odkudkoli. Na vlády roste tlak na další urychlení digitální transformace. Podle článku společnosti Deloitte sedmdesát sedm procent vládních agentur uvádí, že iniciativy digitální transformace prosazované během pandemie již mají pozitivní dopad na jejich organizaci.²

Alcatel-Lucent Enterprise spolupracuje s vládami po celém světě a uznává význam ochrany občanů, operací a budov před kybernetickými a fyzickými riziky. Naše řešení zohledňují bezpečnost a soukromí dat v každé fázi projekčního procesu a jsou vystavěna s volbami odolnosti, aby vyhovovala každému typu organizace. Tato elektronická kniha poskytuje informace o odolnosti a bezpečnosti pro vaše komunikační, cloudová a síťová řešení ALE.

¹ [Kybernetické útoky proti vládám vzrostly v poslední polovině roku 2022 o 95 %, uvádí společnost CloudSek](#). CSO (Úřad pro prevenci konfliktů a stabilizaci) Spojené státy, leden 2023.

² <https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html>.

Elektronická kniha

Upřednostnění odolnosti a bezpečnosti jako priorit

Proč je spolupráce IT/OT (informační technologie/ provozní technologie) kritická

Než prozkoumáme, jak můžete zlepšit odolnost a bezpečnost pomocí řešení Alcatel-Lucent Enterprise, je důležité si uvědomit měnící se vztah mezi informačními technologiemi a provozními technologiemi. Týmy IT a OT v minulosti úzce nespolupracovaly, každý měl své vlastní funkce a odpovědnosti. Tyto dva světy se nyní sbližují a musí fungovat jako jeden. Týmy IT a OT, které si neuvědomují své vzájemné činnosti, nebo které nejsou koordinované a nespolupracují, ohrožují celou organizaci.

Uvažme například obrovské množství zařízení internetu věcí (IoT), která jsou rychle nasazována v mnoha vládních agenturách a chytrých městech. Když tým informační technologie (IT) neví o nových zařízeních IoT implementovaných provozním týmem (OT), nemůže zajistit, aby zařízení vyhovovala bezpečnostním zásadám organizace. Zařízení IoT se dodávají s vysoce variabilními úrovněmi funkcí kybernetické bezpečnosti a nemusí být vybavena nejnovějšími ochrannými mechanismy, nebo jejich schopnosti nemusí být plně implementovány. Tato neautorizovaná „stínová IT zařízení“ mohou používat jakýkoli software a mohou být infikována viry a malwarem. Pokud nejsou kontrolována, mohou do sítě snadno vnést nové zranitelnosti a vektory útoku. Nyní vidíme vznik spolupráce IT/OT potřebné k zajištění bezpečnosti a odolnosti sítě.



Odolná a bezpečná síťová řešení

Síťová infrastruktura je nedílnou součástí fungování vládních organizací a poskytování služeb občanům. Vzhledem k citlivé povaze informací obsažených ve vládních sítích a v kritických službách provozovaných vládami, mohou mít výpadky nebo přerušení síťových služeb vážné důsledky, což z odolnosti a bezpečnosti činí prioritu. Spolehlivé a bezpečné sítě jsou pro vlády zásadní k poskytování účinných veřejných služeb, ochrany citlivých informací a zajištění hladkého provozu.

[Sítě digitálního věku](#) ALE jsou odolné a přesahují rámec toho, co nabízí mnoho dalších poskytovatelů technologií. Bez dodatečných licenčních nákladů začleňujeme bezpečnost do naší sítě a řešení od nejranějších fází projektu.

7 Nejlepších postupů pro vaše síťová řešení

Následuje 7 nejlepších postupů, které zajistí, že plně optimalizujete odolnost a zabezpečení zabudované do vašeho podnikového síťového řešení Alcatel-Lucent.

1. Pravidelně kontrolujte své řešení se svým obchodním partnerem, abyste se ujistili, že jsou nainstalovány nejnovější verze softwaru, záplat a vylepšení bezpečnosti. Výhodou je také nástroj pro správu životního cyklu, jako je ALE PALM, který poskytuje informace o zastarávání a ukončení životnosti. Vládní agentury mohou předem naplánovat výměnu hardwaru a předvídat nasazení.
2. Bezpečný diverzifikovaný kód ALE Secure Diversified Code randomizuje umístění různých segmentů kódu na vašich přepínačích, což dramaticky zvyšuje bezpečnost. Bezpečný diverzifikovaný kód ALE navíc podléhá procesu nezávislého ověřování pravosti a platnosti (IVV) prováděného odborníkem třetí strany na kybernetickou bezpečnost, který analyzuje a testuje operační systém ALE za účelem identifikace a odstranění všech potenciálních zranitelností, zadních vrátek, malwaru nebo zneužití systému, přítomných ve všech nových verzích.
3. Přijměte bezpečnostní strategii [nulové důvěry](#) a implementujte přístup k síti s nulovou důvěrou. Makro- a mikrosegmentace vaší sítě je zásadní pro udržení odolné infrastruktury. Postupujte podle fázovaného přístupu ALE pro mikrosegmentaci, abyste zajistili správnou implementaci tak, aby nezpůsobila rušivé důsledky. [Monitorujte, ověřujte platnost, plánujte, simulujte a prosazujte plnění.](#)
4. Využijte [překlenutí nejkratší cestou Shortest Path Bridging](#) k dosažení redundance prostřednictvím schopnosti dynamicky přesměrovat provoz pomocí více cest v případě selhání jedné cesty. To také vytváří efektivní a automaticky kontejnerizovanou síť.
5. Zvažte využití schopností [virtuálního šasi](#) pro zlepšení spolehlivosti v kritických oblastech, protože to umožňuje redundanci a odolnost vaší sítě, podporuje upgrady softwaru v provozu (ISSU) a umožňuje vyhrazená síťovitá nebo prstencová propojení. Virtuální šasi představuje nákladově efektivní řešení pro zjednodušení správy sítě při zajištění vysoké dostupnosti.
6. Využijte [vlastnosti systému správy sítě Alcatel-Lucent OmniVista®](#). Správce zdrojů OmniVista Resource Manager vám pomůže zajistit, že máte všechny zálohy konfigurace ze síťových přepínačů a budete je moci obnovit pokud by došlo k nejhoršímu nebo v případě potřeby. Tento výkonný nástroj zpracovává celý životní cyklus procesu zálohování a obnovení.
7. Implementujte síťový protokol zvýšení dostupnosti routerů Virtual Router Redundancy Protocol (VRRP). VRRP zvyšuje odolnost sítě tím, že poskytuje záložní virtuální router, který může bezproblémově převzít kontrolu v případě selhání primárního routeru.



Investujte do odolných a bezpečných síťových řešení

Investování do zajištění odolnosti a bezpečnosti vaší sítě má vždy smysl. Pochopení toho, kam nejlépe investovat, však může být složité a vyžaduje čas— klíčem je plánování. Než začnete, uvádíme několik klíčových oblastí, které je třeba zvážit, abyste zajistili bezpečnost a odolnost, které vaše organizace vyžaduje:

- Spolu se svým obchodním partnerem zkontrolujte a aktualizujte projekt sítě, abyste zajistili, že se požadavky vaší organizace projeví v síti, včetně odpovídající úrovně odolnosti pro citlivé a kritické oblasti, které mají dopad na základní vládní služby. V kritických oblastech zvažte přidání záložních serverů a více připojení, pokud je to možné a vhodné.
- Vylepšete reakci na incidenty pomocí funkcí umělé inteligence (AI) a strojového učení (ML) pomocí síťového poradce [Alcatel-Lucent OmniVista Advisor](#). Tento nástroj zajišťuje, že problémy budou vyřešeny dříve, než dopadnou na koncové uživatele a to proaktivní identifikací a zaměřením na problémy se sítí nebo s bezpečností. Urychluje odstraňování problémů a zlepšuje

zabezpečení sítě prostřednictvím auditů konfigurace a správy upozornění v reálném čase na jakékoli náhlé změny chování sítě.

- Zvažte [zesílené přepínače](#) pro drsné prostředí. Tato řada robustně konstruovaných ethernetových přepínačů Alcatel-Lucent Enterprise je speciálně navržena tak, aby vynikala v náročných prostředích a při extrémních teplotách. Tyto přepínače jsou postaveny z robustně konstruovaných komponentů a jsou umístěny v masivních skříních, což zajišťuje trvanlivost a spolehlivost a mají stejný operační systém jako ostatní přepínače ALE. Pro zvýšení bezpečnosti a ochranu citlivých informací jsou některé modely přepínačů vybaveny výstrahami o narušení a poplachovými relé, což umožňuje připojení externích poplachových systémů. Některé modely dokonce podporují MACsec pro bezpečnou datovou komunikaci mezi oběma koncovými pozicemi. Díky možnosti virtuálního šasi v robustně konstruovaných přepínačích můžete získat lepší redundanci, odolnost a škálovatelnost.
- Poskytněte [technické školení ALE](#) pro provozní tým sítě, které jim pomůže rychle odhalovat problémy a reagovat na ně.

Odolná a bezpečná komunikační řešení

Komunikace je zásadní pro to, aby vlády komunikovaly s občany, zúčastněnými stranami a dalšími vládními agenturami, jakož i pro šíření důležitých informací. Komunikační systémy musí být dostupné v době krize, kdy občané nejvíce potřebují vládní pomoc. Odolnost a bezpečnost se vyvíjejí a pravidelné kontroly pomohou udržet vaše komunikační řešení Alcatel-Lucent Enterprise bezpečné a dostupné.

Komunikační řešení ALE jsou bezpečná již svou konstrukcí. To znamená, že bereme v úvahu bezpečnost při každém kroku definování produktu, jeho vývoje a dodávky. Veškerý hardware a operační systémy jsou zesíleny a je zabudována ochrana proti útoku typu Denial of Service (DoS). Dodržujeme uznávané certifikace a akreditace pro globální standardy bezpečnosti a ochrany osobních údajů (ISO 27001, ISO 27017 a ISO 27018). Právě tak se držíme standardů bezpečnosti a ochrany osobních údajů specifických pro obor jako jsou zákon o přenositelnosti zdravotního pojištění a odpovědnosti Health Insurance Portability and Accountability Act (HIPAA) v USA a norma o uchovávání zdravotních údajů Hébergeurs de Données de Santé (HDS) pro hosting zdravotních dat ve Francii, stejně jako regionální normy bezpečnosti ochrany osobních údajů, jako Obecné nařízení o ochrany osobních údajů (GDPR) v Evropské unii.

7 nejlepších postupů pro vaše komunikační řešení

Následuje 7 nejlepších postupů, které vám pomohou zajistit plnou optimalizaci odolnosti a bezpečnosti zabudovaných do vašich komunikačních řešení ALE.

1. Pravidelně kontrolujte stav systému se svým obchodním partnerem, abyste se ujistili, že jsou nainstalovány nejnovější verze softwaru, oprav a vylepšení bezpečnosti a že je vaše smlouva SPS aktuální
2. Pravidelně kontrolujte komponenty zabezpečení a kontinuity služeb ve vašem systému správy sítě [Alcatel-Lucent OmniVista 8770](#), který obsahuje cenné informace o odolnosti a bezpečnosti a o funkcích pro vaše komunikační řešení.
 - Zvažte automatizované vzdálené zálohování systému, abyste zabránili ztrátě konfiguračních dat
 - Nakonfigurujte monitorování alarmu a zajistěte, aby byl pravidelně aktualizován se správnými prahovými hodnotami. Dále ověřte, zda jsou příslušným osobám zasílána oznámení o selhání komunikačního systému nebo upozornění na kvalitu.
3. Zkontrolujte a prosazujte zásady silného hesla, nejlépe pomocí externího ověřování (server RADIUS) a nastavte připomenutí uživatelům, aby se zabránilo telefonním podvodům Toll Fraud, které jsou v mnoha zemích stále hrozbou
4. Školte zaměstnance a ujistěte se, že jsou si vědomi rizik a preventivních opatření
5. Zkontrolujte stav, vhodnost a provozuschopnost aplikačních serverů kritických pro podnikání
6. Zvažte specifické VLAN pro hlas. Oddělením hlasu od jiného provozu se snižuje pravděpodobnost kontaminace, která by mohla narušit provoz a potenciálně vládní služby.
7. Zkontrolujte, zda jsou správně nastaveny hraniční řadiče relací (SBC). Požadavky se v průběhu času mohly změnit



Investujte do odolných a bezpečných komunikačných řešení

V posledních několika letech globální prostředí nasměřovalo pozornost na důležitost komunikace mezi vládou a občany. Níže jsou uvedeny některé klíčové oblasti, které je třeba zvážit pro vládní agentury plánující investovat do komunikačních řešení za účelem zvýšení odolnosti a bezpečnosti.

- Redundantní a odolná architektura. Vaše architektura by měla být plně redundantní a odolná. Duplikování serverů zpracování hovorů v kritických oblastech, implementace redundance vzdálené lokality a duplikace kritických aplikačních serverů může poskytnout další ochranu.
- Zákazníci, kteří používají [TDM DECT](#), by měli zvážit rozšíření pokrytí do kritických oblastí, aby zajistili odolnost v případě selhání systému IP
- Vytvořte pracovní postup s pomocí Rainbow a/nebo asistenta [Alcatel-Lucent Visual Notification Assistant](#) (VNA) s automatickými spouštěči (spouštěč je člověk, IoT nebo systém), abyste upozornili klíčové lidi na problémy se systémem, aby jednali rychle a urychlili proces obnovy
- Nasaďte silné šifrování. Šifrování je založeno na průmyslových standardech projektovaných nativně do řešení, bez jakéhokoli dopadu na kvalitu a výkon hlasu



- Implementujte [Rainbow™ od společnosti Alcatel-Lucent Enterprise](#), ideální nástroj pro spolupráci, který doplňuje komunikační řešení ALE. Rainbow nabízí komplexní sadu funkcí včetně hlasu, videa a okamžitých zpráv, které umožňují bezproblémovou komunikaci a efektivní spolupráci. S pomocí Rainbow si můžete vyměňovat obrázky, videa a kanály pro video dohled, zvyšovat kontextové povědomí a umožnit lepší rozhodování. Rainbow také poskytuje hybridní komunikaci se zabezpečeným připojením mezi místními zařízeními a cloudem. Zajišťuje odolnou komunikaci, udržuje vás ve spojení s kolegy a zákazníky užívajícími Rainbow a poskytuje nepřerušované připojení i v náročných situacích. Hybridní komunikace má také výhodu, že cloudové a místní operace jsou provozovány z různých míst pro maximální odolnost, aby komunikace zůstala otevřená.
- Pro agentury s přísnějšími bezpečnostními požadavky nabízí Rainbow Edge místní alternativu s instancí privátního cloudu. Instance může být hostována v jakémkoli datovém centru a poskytuje úplnou kontrolu nad servery, úložišti a sítěmi, což agenturám umožňuje přizpůsobit a konfigurovat infrastrukturu podle svých požadavků. Lze implementovat personalizované zásady bezpečnosti a zdroje lze spravovat autonomně. Tato úroveň kontroly poskytuje úplnou viditelnost a autoritu nad infrastrukturou, což agenturám umožňuje činit informovaná rozhodnutí a optimalizovat výkon v souladu s jejich cíli.
- Definujte bezpečnou distribuovanou komunikační strategii pracovní síly. ALE poskytuje četné možnosti komunikace a spolupráce pro zaměstnance distribuované, zaměstnance mobilní a zaměstnance pracující z domova, včetně následujícího:
 - Rainbow
 - [Softphone \(software telefonie\) pro stolní zařízení přes IP](#)
 - [Softphone ALE](#)
 - [Stolní telefon s vestavěnou VPN a lze hromadně nasadit s vestavěným zabezpečením \(VPN\)](#)

Ochrana lidí a aktiv

ALE nabízí flexibilní, bezpečné a vysoce dostupné systémy komunikace v reálném čase a [oznamovací systémy](#). Tato řešení se mohou integrovat do provozu veřejné bezpečnosti nebo inteligentních městských řídicích center, zefektivnit dispečink a stanovení priorit hovorů, usnadnit kontextovou výměnu informací s daty IoT a zlepšit úsilí o spolupráci mezi orgány první reakce na mimořádné události a různými zúčastněnými stranami, což umožní lepší rozhodování a koordinaci.

Schopnost propojit zařízení IoT v budovách, místech a městech v kombinaci s analytikou a umělou inteligencí zásadně mění komunikační prostředí. Díky integraci senzorů, video dohledu, průběhu práce Rainbow a AI je možný přechod od přístupu reaktivního k přístupu proaktivnímu, což zvyšuje efektivitu procesů z hlediska času a nákladů. Tato integrace usnadňuje komplexní pochopení kontextu, podporuje rozhodovací procesy a následně zkracuje dobu reakce na mimořádné události. Funkce, jako je sledování aktiv a ovládání inteligentních zámků a osvětlení, navíc zefektivňují provoz. Schopnost zaznamenávat komunikaci a zaznamenávat akce navíc zjednodušuje následnou analýzu po události, zlepšuje bezpečnostní procesy a zmírňuje potenciální závazky. K dosažení těchto pokroků je klíčové propojené prostředí s všudypřítomným přístupem k Wi-Fi a snadným připojením IoT.

Pro časově citlivé, bezpečné a vysoce dostupné platformy komunikace v reálném čase je robustní infrastruktura nezbytná pro zajištění bezproblémového provozu. Vaše technologická infrastruktura by měla zahrnovat vhodný software, síťové protokoly s vysokou dostupností a flexibilitu pro začlenění robustně konstruovaných síťových přepínačů, které se mohou bezproblémově integrovat do vašeho ekosystému a odolávat drsným podmínkám prostředí, včetně omezeného proudění vzduchu, otřesů a teplot extrémního počasí. Volba robustně konstruovaného vybavení zajišťuje dlouhou životnost v tak náročných místech, kde by nerobustní zařízení byla méně trvanlivá.

V oblasti systémů fyzické bezpečnosti je v sázce mnoho. Každá minuta a každý kousek videozáznamu může být pro úřady zásadní při identifikaci provinění, určení zdroje incidentu nebo pochopení příčiny katastrofy. Robustní [infrastruktura video dohledu](#) je zásadní. Síťová infrastruktura by měla nejen poskytovat dostatečnou šířku pásma a napájení přes Ethernet (PoE) pro kamery dohledu, ale také bezproblémově integrovat se systémy správy video dohledu. Tato integrace zajišťuje efektivní a spolehlivou síť dohledu s hladkým provozem a snadným řešením problémů. Provozní tým by měl být schopen rychle vyřešit jakékoli problémy s videem, zejména v prostředích, kde je každý snímek videa kritický. [Integrace řešení Alcatel-Lucent OmniSwitch®](#) realizovaná prostřednictvím pluginů s hlavními systémy správy videa, vám umožní dosáhnout tohoto důležitého cíle.

Kromě toho existují situace, kdy je nutné sledovat aktiva nebo lokalizovat jednotlivce nebo vybavení ve vaší organizaci. Efektivní řešení pro sledování aktiv se spoléhá na jeho schopnost snadno a přesně lokalizovat lidi a aktiva. Takový systém také zvyšuje bezpečnost a zabezpečení tím, že umožňuje rychlé odeslání pomoci, když je známo umístění jednotlivců. S řešením [Alcatel-Lucent OmniAccess® Asset Tracking lze](#) personál a vybavení rychle lokalizovat a zobrazit na mapě prostorového uspořádání. Sledování aktiv také poskytuje informace o vzorcích využití. Vědět, zda jsou aktiva využívána příliš nebo nedostatečně, může poskytnout cenné informace.



Nezávislost a bezpečnost dat

Alcatel-Lucent Enterprise překonává jiné poskytovatele technologie v implementaci nejlepších postupů potřebných pro komplexní kybernetickou bezpečnost. V ALE:

- Dodržujeme nejlepší postupy a doporučení Národního institutu vědy a techniky (NIST) při provádění hodnocení rizik nových funkcí a při implementaci funkcí kybernetické bezpečnosti v našich řešeních, jako je nativní šifrování
- Máme certifikaci Common Criteria EAL2+.
- Uplatňujeme normy ISO 27001 na všechna naše řešení založená na cloudu
- Podporujeme systém ZTNA, granulární segmentaci sítí a vysoce specifické bezpečnostní zásady v zájmu snížení rizika neoprávněných činností

- Provádíme na všech našich produktech vysoce specializované testy zaměřené na zabezpečení, jako jsou testy průniku.
- Zajišťujeme, aby naše produkty získaly klíčové oborové certifikace, jako jsou HDS, HIPAA a FERPA (zákon o rodinných právech na vzdělávání a ochraně soukromí).

Jako uznávaní odborníci na kybernetickou bezpečnost přispíváme k návrhům Evropské unie na směrnice týkající se kybernetické bezpečnosti. Naše odborné znalosti kybernetické bezpečnosti využíváme také k tomu, abychom pomohli našim zákazníkům vybrat si a implementovat správnou kombinaci bezpečných řešení pro jednotnou komunikaci a spolupráci podle jejich potřeb a školíme jejich zaměstnance v nejlepších postupech kybernetické bezpečnosti.

