



Zabezpečení řešení pro jednotnou komunikaci a spolupráci

Co to znamená v dnešním měnícím se světě

Bílá kniha

Alcatel·Lucent 
Enterprise

Obsah

- | Větší zaměření na kybernetickou bezpečnost
- | Šest klíčových oblastí pro komplexní kybernetickou bezpečnost
- | Dosažení obchodních cílů s menšími riziky
- | Kybernetická bezpečnost: Zabudovaná do smýšlení poskytovatele technologií

Větší zaměření na kybernetickou bezpečnost

V průběhu několika posledních let téměř všechny podniky a vládní organizace změnily způsob, jakým jejich zaměstnanci komunikují, spolupracují a sdílejí informace. Zatímco rychlý přechod na podporu zaměstnanců pracujících z domova byl zásadní pro udržení návaznosti podnikání během pandemie, vybral si svou daň: Obvod sítě nyní přesahuje hranice tradičních kanceláří, čímž výrazně zvětšuje plochu organizace náchylnou na útok.

Rizika spojená s větším obvodem sítě v dohledné době nezmizí. Podle společnosti Gartner bude 39 procent pracovníků z celého světa, jejichž hlavním kapitálem jsou znalosti, do konce roku 2023 pracovat v hybridních dálkových a kancelářských modelech. Ve Spojených státech toto číslo stoupá na 51 procent¹.

Geopolitické nepokoje dále zvýšily rizika kybernetické bezpečnosti. Agentura Evropské unie pro kybernetickou bezpečnost označila ruskou invazi na Ukrajinu za „událost, která mění celou situaci“ pro globální kybernetickou doménu.² Podle Asociace ukrajinských IT outsourcingových společností se jedna z pěti společností v žebříčku Fortune 500 v roce 2022 spoléhala na vývojáře softwaru v dané zemi.³

Současně se zvyšuje společenský dopad kybernetických útoků. V roce 2022 jsme zaznamenali velké kybernetické útoky na klíčovou občanskou infrastrukturu, které způsobily národní pohotovost v Kostarice⁴, a pokračující cílení na organizace poskytující zdravotní péči.⁵

Organizace si nemohou dovolit zlepšení kybernetické bezpečnosti odkládat

Odhaduje se, že kybernetická kriminalita v roce 2021 stála globální ekonomiku 5,5 bilionu EUR, ale očekává se, že do roku 2025 škody překročí 10 bilionů EUR.⁶ Tento problém je tak závažný, že Evropská unie vytváří zákon o kybernetické odolnosti a vydala výrazně vylepšenou verzi 2 své směrnice o bezpečnosti sítí a informací (NIS), aby ochránila spotřebitele a podniky, které nakupují nebo používají produkty nebo software s digitální součástí.⁷ USA rovněž zavádějí opatření na posílení kybernetické bezpečnosti, včetně výkonného nařízení 14028, které vybízí agentury, aby přijaly zásady kybernetické bezpečnosti s nulovou důvěrou a odpovídajícím způsobem upravily síťové architektury.⁸

Pokud se podniky a vlády chtějí digitálně transformovat a trvale podporovat flexibilní pracovní modely, nemají jinou možnost než posílit kybernetickou bezpečnost. Řešení, která jejich týmy používají ke komunikaci, spolupráci a sdílení informací, musí zahrnovat osvědčené postupy kybernetické bezpečnosti na všech úrovních a ve všech aspektech funkčnosti.

¹ Společnost Gartner předpovídá, že 39 % pracovníků na celém světě, jejichž hlavním kapitálem jsou znalosti, bude do konce roku 2023 pracovat hybridně. Gartner, březen 2023.

² Nestabilní geopolitická situace otřásá trendy prostředí hrozeb kybernetické bezpečnosti 2022. Agentura Evropské unie pro kybernetickou bezpečnost, listopad 2022.

³ Jedna z pěti společností v žebříčku Fortune 500 spoléhá v oblasti svých požadavků na vývoj softwaru v roce 2022 na Ukrajinu. Ukrajinská hi-tech iniciativa, říjen 2022.

⁴ 13 nejdražších kybernetických útoků roku 2022: ohlédnutí. Bezpečnostní zpravodajství, prosinec 2022.

⁵ Recenze roku 2022: rušný rok v oblasti kybernetické bezpečnosti. Forbes, prosinec 2022.

⁶ Nový návrh Evropské unie pro kybernetickou bezpečnost se zaměřuje na počítačovou kriminalitu. Světové ekonomické fórum, září 2022.

⁷ Zákon EU o kybernetické odolnosti. Evropská komise, září 2022.

⁸ Výkonná nařízení o zlepšení národní kybernetické bezpečnosti. Agentura pro kybernetickou bezpečnost a bezpečnost infrastruktury.

Bílá kniha

Zabezpečení řešení pro jednotnou komunikaci a spolupráci





Šest klíčových oblastí pro komplexní kybernetickou bezpečnost

Řešení pro jednotnou komunikaci a spolupráci musí zavést kompletní kybernetické zabezpečení, protože je to jediný způsob, jak zajistit, aby bylo zabezpečení aplikováno v maximální možné míře. Komplexní přístup ke kybernetické bezpečnosti pomáhá podnikům a vládám v následujících oblastech.

- **Zabránit kybernetickým útokům** díky zavedení kybernetické bezpečnosti ve všech aspektech návrhu produktu, což snižuje plochu náchylnou na útoky.
- **Ochrana před kybernetickými útoky** implementací nejnovějších bezpečnostních standardů a osvědčených postupů ve všech součástech řešení v zájmu zvýšení odolnosti.
- **Reagování na kybernetické útoky** přijetím rychlých a vhodných opatření, jejichž cílem je omezení dopadu a zlepšení odolnosti, pokud dojde k útoku.

Aby bylo možné určit, zda řešení pro jednotnou komunikaci a spolupráci implementují kybernetickou bezpečnost v maximální možné míře, měla by být provedena hodnocení řešení v níže popsaných oblastech. Zaměření na tyto oblasti může pomoci zajistit komplexní hodnocení řešení a zároveň se zaměřit na klíčová zranitelná místa v celém prostředí kybernetických hrozeb.

1 Zabezpečení již od samotného návrhu

Většina návrhů řešení dříve vycházela z potřeby nových funkcí. Bezpečnost byla sice důležitá, ale až sekundární aspekt. S měnícím se prostředím se tradiční priority návrhu obrátily a návrhy řešení musí nyní musí vycházet z požadavků na kybernetickou bezpečnost.

Hardwarová a softwarová řešení, která jsou bezpečná už ze své podstaty, berou v úvahu bezpečnost při každém kroku definice, vývoje a dodání produktu. U veškerého hardwaru a operačních systémů je zabezpečení posíleno, má zabudovanou ochranu Denial of Service (DoS, Odepření služby) a řešení implementují osvědčené postupy v oblasti kybernetické bezpečnosti, které jsou pro toto odvětví nejdůležitější. Například řešení pro jednotnou komunikaci a spolupráci pro organizace vnitrostátní bezpečnosti splní velmi vysoké standardy odolnosti a důvěrnosti, které tyto organizace vyžadují.

2 Zabezpečení přístupu k síti s nulovou důvěrou

Strategie zabezpečení, které poskytují důvěru na základě umístění uživatele uvnitř firemního firewallu, přihlašovací údaje, které zadávají, nebo aplikace či zařízení, které používají, již nejsou adekvátní – i když je zkombinováno více bezpečnostních mechanismů. Žádnému uživateli, zařízení nebo aplikaci by se dnes nemělo implicitně důvěřovat.

Řešení pro jednotnou komunikaci a spolupráci, která zavádějí bezpečnostní model ZTNA (Zero Trust Network Access, přístup k síti s nulovou důvěrou), pomáhají organizacím účinně čelit neustále se vyvíjejícím hrozbám. ZTNA nedůvěřuje žádnému uživateli, zařízení ani aplikaci, a to bez ohledu na to, kde se nachází. Je založen na pěti klíčových prohlášeních:

- Síť je nepřátelská.
- Interní a externí hrozby jsou všudypřítomné.
- Poloha k určení důvěryhodnosti nestačí.
- Každý přístroj, uživatel a síťový tok musí být ověřen a autorizován.
- Zásady sítě a zabezpečení musí být dynamické a musí používat co nejvíce zdrojů dat.



3 Makrosegmentace a mikrosegmentace

Makrosegmentace a mikrosegmentace umožňují podrobný a vysoce kontrolovaný přístup ke kybernetické bezpečnosti pro všechny různé uživatele, zařízení a aplikace, které mají přístup k síti.

Makrosegmentace odděluje uživatele, zařízení a aplikace podle jejich funkční domény, takže nemohou komunikovat s prvky v jiných makrosegmentech. Například aplikace jednotné komunikace a spolupráce v jednom makrosegmentu nemohou komunikovat s bezpečnostními technologiemi, jako jsou bezpečnostní kamery a systémy zamykání dveří ve druhém makrosegmentu nebo senzory a ovládací prvky pro osvětlení, vytápění a klimatizaci ve třetím makrosegmentu.

Mikrosegmentace definuje, jak mohou uživatelé, zařízení a aplikace v makrosegmentu vzájemně komunikovat, a obvykle se řídí velmi specifickými bezpečnostními zásadami. Například bezpečnostní kamera by neměla mít možnost propojení se zámkem dveří, přestože se nacházejí ve stejném makrosegmentu souvisejícím s bezpečností.

4 Komplexní nativní šifrování

V moderních organizacích se mohou zaměstnanci, zákazníci, partneři a dodavatelé nacházet kdekoli na světě. Řešení, která používají ke komunikaci a spolupráci, mohou být instalována v budově, ve které pracují, na druhé straně města, nebo v datovém centru na druhé straně světa. V každém případě musí být lidé schopni si bezpečně a důvěrně vyměňovat informace pomocí hlasu, videa a textu.

Aby bylo zajištěno, že k vyměňovaným informacím budou mít přístup pouze účastníci konverzace, musí být každá konverzace plně šifrována od počátku až do cíle. To znamená, že každý hardwarový a softwarový prvek zapojený do komplexní komunikace musí mít šifrovací mechanismy, které do nich nativně zabudovaly bezpečnostní agentury.

5 Certifikace a akreditace bezpečnosti a ochrany osobních údajů

Jen před několika lety byly nejpřísnější bezpečnostní certifikace a akreditace vyžadovány pouze pro bezpečnostní produkty, jako jsou brány firewall, nebo v konkrétních odvětvích, jako je obrana. V současné době musí být bezpečnostní normy uplatňovány na všechny technologické produkty ve všech odvětvích.

Je nesmírně důležité ověřit, zda jsou nároky na kybernetickou bezpečnost podloženy uznávanými certifikacemi a akreditacemi. Zde je několik příkladů předpisů, které je třeba hledat:

- **Globální standardy bezpečnosti a ochrany soukromí**, jako je ISO 27001 pro bezpečnost informací, ISO 27017 pro bezpečnější a zabezpečenější cloudová prostředí, ISO 27018 pro ochranu osobních identifikačních údajů v cloudových prostředích a Common Criteria Evaluation Assurance Level (EAL) 2 a vyšší pro zabezpečení počítačového systému
- **Standardy bezpečnosti a ochrany soukromí specifické pro dané odvětví**, jako je zákon o odpovědnosti za přenos údajů o zdravotním pojištění (HIPAA) v USA a Hébergeurs de Données de Santé (HDS) pro hostování zdravotních údajů ve Francii
- **Regionální normy bezpečnosti a ochrany soukromí**, jako je obecné nařízení o ochraně osobních údajů (GDPR) v Evropské unii

6 Průběžné, specializované testování zabezpečení

Stejně jako standardy zabezpečení, i specializované procesy testování zabezpečení, které bývají dříve vyhrazeny pro bezpečnostní produkty, jsou nyní povinné v řešeních pro jednotnou komunikaci a spolupráci.

Testy průniku jsou toho ukázkovým příkladem. Tyto testy simulují kybernetické útoky, aby odhalily chyby zabezpečení, aby je bylo možné proaktivně řešit dříve, než nastanou problémy. Aby bylo možné udržet náskok před kybernetickými hrozbami v neustále se měnícím prostředí, testy průniku, které vychází výhradně z požadavků na kybernetickou bezpečnost, musí být prováděny průběžně.

Poskytovatelé technologií, kteří svým zákazníkům pomáhají udržovat maximální kybernetickou bezpečnost, musí poskytnout zdroje, nástroje a odborné znalosti potřebné k provádění nepřetržitého testování průniku.



Dosažení obchodních cílů s menšími riziky

Řešení pro jednotnou komunikaci a spolupráci, která implementují kompletní řadu opatření v oblasti kybernetické bezpečnosti popsaných v předchozí části, poskytují podnikům a vládním organizacím svobodu a flexibilitu při prosazování činností a současně minimalizují rizika a zajišťují soulad s předpisy. Mohou:

- **Podpořit zaměstnance**, aby bezpečně a důvěrně spolupracovali a sdíleli informace prostřednictvím jakéhokoli média a zařízení a z libovolného místa
- **Zlepšit zkušenosti zákazníků** díky bohatší, informativní a zajímavé komunikaci, rychlejšímu rozhodování, automatizovaným obchodním procesům a schopnost proaktivně odhalovat problémy dříve, než se zákazníka dotknou
- **Zvýšit provozní dokonalost a pružnost** pomocí digitální infrastruktury, která je nasazena tam, kde má pro organizaci největší smysl — na místě nebo v hybridním, soukromém nebo veřejném cloudu – při současném dodržení přísných zásad ochrany osobních údajů a zajištění souladu s předpisy o ochraně osobních údajů

Tyto příklady ukazují jen několik příležitostí, které jsou možné a které lze snadno přizpůsobit dalším požadavkům a odvětvím.

Vytvoření flexibilního digitálního pracoviště pro posílení postavení zaměstnanců

Se správnou kombinací řešení zabezpečené komunikace a spolupráce mohou zaměstnanci pracovat rychleji, flexibilněji a současně v plné míře dodržovat oborové předpisy.

- **Ve zdravotnictví** mohou pracovníci, kteří jsou často v pohybu, spolupracovat a sdílet informace a přitom v plné míře dodržovat standardy zabezpečení dat. Zaměstnanci si mohou snadno vyměňovat nové informace a rychle získat potřebnou pomoc. Zdravotnický personál může používat zabezpečenou komunikaci v reálném čase ke zlepšení výsledků pacientů a efektivity pracovních postupů. Nezdravotnický personál může urychlit procesy a reakce na problémy s údržbou, které by mohly ovlivnit bezpečnost pacientů a zaměstnanců.
- **Ve vzdělávání** mohou učitelé poskytovat bohatší a zajímavější zkušenosti s učením na dálku a studenti budou mít více příležitostí účastnit se aktivit, spolupracovat na projektech a komunikovat pomocí preferovaného média. Komplexní řízení přístupu a automatizované zásady udržují integritu dat a analytika stanovuje priority pro důležitou komunikaci a síťové zdroje.
- **Ve vládních organizacích** si zaměstnanci mohou bezpečně vyměňovat informace mezi různými rozptýlenými týmy. Mohou sdílet obrazovky, na dálku ovládat pracovní plochu někoho jiného a vyměňovat si velké soubory, což přispívá k lepší spolupráci. Navíc mohou bezpečně komunikovat s občany prostřednictvím webových nebo mobilních aplikací využívajících hlas, video, chat nebo rychlé zprávy.
- **V dopravě** digitální pracoviště umožňuje zaměstnancům používat při práci vlastní zařízení, zavádět efektivnější procesy a poskytovat cestujícím lepší služby, jako je možnost pracovat při cestování. Zabezpečené komunikační protokoly, zesílené instalace a diverzifikovaný kód chrání data všude v síti.

Vše propojte a nabídněte zákazníkům to nejlepší

Bezpečné propojení lidí, objektů a aplikací pomocí komunikace v reálném čase umožňuje podnikům a vládním organizacím:

- Poskytnout zaměstnancům zařízení, technologie a data, která potřebují k lepší podpoře zákazníků, a zároveň minimalizovat riziko, že lidská chyba nebo nedostatek uvědomění ohrozí bezpečnost
- Používat integrovaná, zabezpečená zařízení ke komunikaci a spolupráci s klienty na cestách, s plným přístupem k řešením pro správu vztahů se zákazníky (CRM)
- Zvýšit ochranu, kontrolu a přehled nad rychle rostoucí a rozmanitou škálou zařízení IoT (Internet věcí)
- Udržovat systémy pro komunikaci a spolupráci aktuální, aby bylo možné předejít riziku, že zastaralé aplikace zvýší plochu pro útoky a odhalí zranitelná místa
- Implementovat efektivní řízení přístupu a komplexní šifrování ve všech platformách

Jednotná správa sítě umožňuje celostní správu všech komunikačních platforem, aplikací a zařízení IoT. Jednotná správa sítě:

- Zjednodušuje úlohy správy napříč kabelovými a bezdrátovými sítěmi a zařízeními IoT, aby bylo možné snížit náklady na správu sítě, optimalizovat výkon sítě a zvýšit provozní účinnost.
- Zrychluje řešení problémů ve stále rozmanitějších technologických prostředích, aby bylo možné snížit riziko přerušení provozu a prostojů.

Jednotná správa sítě napříč odvětvími poskytuje celou řadu výhod. Například:

Ve zdravotnictví mohou řešení IoT sledovat umístění kritických zařízení, jako jsou kyslíkové nádoby, resuscitační vozíky, monitory pacientů, držáky na infuze a invalidní vozíky, což zvyšuje bezpečnost a účinnost. Propojení mezi lidmi, objekty a aplikacemi lze také využít ke spuštění alarmů, které varují zdravotnický personál na potřeby pacienta nebo poruchy zařízení a mohou upozornit každého v zařízení o nebezpečné situaci.

Ve vzdělávání vzniká nový potenciál – propojit zařízení a aplikace chytrého kampusu s více vrstvami zabezpečení, aby bylo možné ochránit prostředky instituce před nedostatečně zabezpečenými zařízeními, která mají přístup k síti. Vzdělávací instituce mohou také použít otisky prstů zařízení IoT k identifikaci charakteristik zařízení, jako je typ, výrobce, model a operační systém, což zjednodušuje a urychluje nastavení sítě IoT a zavedení zařízení.



Zvyšte provozní dokonalost a pružnost

Díky flexibilitě bezpečného nasazení jednotných řešení pro komunikaci a spolupráci na místě nebo v hybridním, soukromém nebo veřejném cloudu mohou podniky a vládní organizace těžit z digitálních technologií způsobem, který je v souladu s jejich cíli a motivacemi. Každá organizace může dosáhnout nové úrovně provozní dokonalosti a současně splnit požadavky specifických pro dané odvětví, když přijme cloudové modely za účelem zlepšení provozu a pružnosti, například:

- **Zdravotní péče**, kde lze digitální záznamy využít ke zlepšení péče o pacienty a zvýšení efektivity s plnou důvěrou, že osobní údaje jsou uloženy v zabezpečeném a certifikovaném datovém centru v cloudu
- **Vzdělání**, kde fakulta, zaměstnanci a studenti mají odkudkoli bezpečný přístup ke cloudovým aplikacím a službám, který bere ohledy na ochranu soukromí. A IT oddělení mohou zkrátit čas a snížit náklady spojené s nasazením, podporou a modernizací široké škály aplikací.
- **Vláda**, kde lze důvěrnou komunikaci podporovat prostřednictvím vysoké dostupnosti a chránit pomocí vestavěných mechanismů DoS a hardwaru a operačních systémů se zesíleným zabezpečením
- **Doprava**, kde změna možností komunikace může vést k nebezpečným situacím, kvůli čemuž jsou odolná řešení pro řízení dat zcela klíčová

Kybernetická bezpečnost: Zabudovaná do smýšlení poskytovatele technologií

I když mnoho poskytovatelů technologií kybernetickou bezpečnost zdůrazňuje, ne všichni mají komplexní odborné znalosti, aby mohli zavést komplexní zabezpečení.

Společnost Alcatel-Lucent Enterprise dělá mnohem víc než ostatní poskytovatelé, aby implementovala všechny osvědčené postupy potřebné pro komplexní kybernetickou bezpečnost. My:

- Při provádění hodnocení rizik nových funkcí a zavádění funkcí kybernetické bezpečnosti, jako je nativní šifrování, v našich řešeních dodržujeme osvědčené postupy a doporučení Národního institutu vědy a techniky (NIST).
- Máme certifikaci minimálně Common Criteria EAL2+.
- Uplatňujeme normy ISO 27001 na všechna naše cloudová řešení.
- Podporujeme systém ZTNA, granulární segmentaci sítí a vysoce specifické bezpečnostní zásady v zájmu snížení rizika neoprávněných činností.
- Provádíme vysoce specializované testy zaměřené na zabezpečení, jako jsou testy průniku, na všech našich produktech.
- Zajišťujeme, aby naše produkty získaly důležité oborové certifikace, jako je HDS, HIPAA a FERPA zákon o rodinných právech na vzdělávání a ochraně soukromí, jako Rainbow by Alcatel-Lucent Enterprise.

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

Další informace

Chcete-li zjistit, jak můžeme vaší organizaci pomoci plně využít bezpečných řešení Komunikace digitálního věku, [navštivte naše webové stránky](#) nebo [nás kontaktujte ještě dnes](#).

Společnosti Alcatel-Lucent Enterprise důvěřují lidé z celého světa

Přední organizace z různých oborů se spoléhají na naše bezpečné řešení Komunikace digitálního věku k dosažení svých cílů, mezi které patří také následující:

- [Metropole a město Perpignan](#) ve Francii, kde vládní úředníci zavádějí strategický plán digitální transformace, který zahrnuje videokonference a hlasovou komunikaci pro zaměstnance, podporu aplikací IoT a nový obsah a služby pro obyvatele Perpignanu, turisty a obecní zaměstnance
- [Newman University](#) v USA, katolická vysoká škola svobodných umění, která poskytla zaměstnancům funkce mobilních telefonů, které nevyžadují přímá telefonní čísla, a IT tým s jedinou, intuitivní, cloudovou platformou pro správu, poskytování a sledování veškeré sítové infrastruktury
- [Nemocnice Kingsway](#) v Indii, která zavedla řešení infrastruktury komunikace v reálném čase, která zachovávají spojení mezi klinickými a administrativními pracovníky, aby bylo možné optimalizovat poskytování péče a nabídnout pacientům lepší zkušenosti
- [J. Malucelli Group](#) v Brazílii, která modernizovala svou síť konvergováním hlasovým a datovým řešením, které zahrnuje cloudový telefonický přenos i síť LAN a Wi-Fi se správou cloudu, aby bylo možné zjednodušit komunikaci a snížit náklady na komunikaci pro několik společností ve skupině.

