



Budování nákladově efektivní sítě s nulovou důvěrou

Maximalizujte zabezpečení sítě a minimalizujte náklady.



Kybernetická bezpečnost a nulová důvěra

Kybernetická bezpečnost je stále důležitější otázkou, protože technologie se stále vyvíjí a počet a složitost kybernetických hrozeb stále roste. Existují rychle se vyvíjející hrozby, díky nimž je pro organizace náročné je předvídat a bránit se proti nim, což vyžaduje, aby odborníci na kybernetickou bezpečnost měli přehled o nejnovějších trendech a zranitelných místech.

S mnoha různými zdroji a kanály útoků, jako jsou phishingové e-maily, sociální inženýrství a softwarové zranitelnosti, vyžaduje obrana proti kybernetickým hrozbám pro každý typ útoku jedinečný přístup.

Identifikace a ochrana všech potenciálních zranitelností v komplexním systému mohou být náročné, takže pro odborníky na kybernetickou bezpečnost je zásadní pochopit, jak různé systémy a sítě spolupracují, aby mohli vyvinout účinná bezpečnostní opatření.

Běžnou příčinou narušení kybernetické bezpečnosti bývá lidská chyba a do roku 2025 se odhaduje, že nedostatek talentovaných pracovníků nebo lidské selhání budou zodpovědné za více než polovinu závažných kybernetických incidentů.¹

Splnění složitých předpisů a norem kybernetické bezpečnosti, jako je obecné nařízení o ochraně osobních údajů (GDPR) a zákon o odpovědnosti za přenos údajů o zdravotním pojištění (HIPAA), je dalším problémem, který vyžaduje odborné znalosti.

1 Předpovědi společnosti Gartner® pro rok 2023: Obor kybernetické bezpečnosti se zaměřuje na lidské dohody | Bitsight, leden 2023.

Přehled řešení

Budování nákladově efektivní sítě s nulovou důvěrou



Proces narušení kybernetické bezpečnosti

Následující obrázek ukazuje fáze, které kybernetický útočník provádí, aby pronikl do sítě a ukradl cenná data. Začíná to průzkumem, kdy útočníci zkoumají, identifikují a vybírají cíle a hledají zranitelnosti sítě.

Další fází je zbrojení, kdy útočníci určují, jak cílový koncový bod ohrožit a jak doručit ozbrojenou nálož.

Poté přichází zneužití, kdy útočník aktivuje ozbrojenou nálož a eskaluje oprávnění na kompromitovaném koncovém bodě, aby se po síti laterálně pohyboval.

Další fází je instalace, kdy útočníci vytvářejí vzdálený přístup k prostředí a instalují malware, aby v síti mohli zůstat.

Ve fázi řízení a kontroly útočníci vytvářejí šifrované komunikační kanály vedoucí zpět na velící a řídicí servery, aby vzdáleně nasměrovali útok a splnili cíle.

Poslední fází je boční pohyb a exfiltrace, kdy útočníci mohou mít více cílů, včetně krádeže dat, zničení nebo úpravy kritických systémů a odmítnutí služeb.

Klíčem k zastavení útočníků je včasné odhalení různých fází životního cyklu útoku a narušení jejich postupu.

Abyste tomu zabránili, musíte provést řadu opatření, jako je správa zranitelností a oprav, detekce a prevence malwaru, blokování rizikových aplikací a služeb a protokolování a monitorování všech sítí, koncových bodů a samozřejmě cloudové aktivity.

Na straně sítě je třeba implementovat technologie, které poskytují podrobné řízení aplikací a monitorují provoz mezi zónami nebo segmenty v modelu nulové důvěry. Nulová důvěra funguje na principu, že ve výchozím nastavení by vše mělo být považováno za nedůvěryhodné.

Tento koncept nulové důvěry byl vyvinut v reakci na rostoucí počet promyšlených kybernetických útoků na počítačové sítě. Organizace obvykle při ochraně sítě spoléhají na bezpečnostní řešení na obvodu, jako jsou brány firewall a antivirový software. Vzhledem k tomu, že jsou kybernetické útoky stále pokročilejší a složitější, tato obvodová řešení se ukázala jako nedostatečná a místo toho musí být každý požadavek na přístup ověřen a potvrzen, než bude udělen přístup ke zdrojům.



Zdroj: [XDR for Dummies, Palo Alto Networks Special Edition, 2022](#)

Přehled řešení

Budování nákladově efektivní sítě s nulovou důvěrou



Posílení strategie nulové důvěry

Společnost Alcatel-Lucent Enterprise pomáhá zákazníkům k lepšímu zabezpečení a přejít k jednoduchému a nákladově efektivnímu prostředí s nulovou důvěrou. Ve společnosti ALE chápeme důležitost implementace modelu nulové důvěry v zájmu zajištění bezpečnosti sítí a dat našich klientů. Nabízíme řadu řešení, která organizacím pomohou zavést síť s nulovou důvěrou a řešit problémy, které představují kybernetické hrozby.

Posílení sítě

Nabízíme **zesílenou síť – zevnitř i zvenčí**. Začíná to bezpečnou infrastrukturou a zajištěním toho, že samotné zařízení nebude ohroženo. Naše řada produktů [Alcatel-Lucent OmniSwitch®](#) běží na zabezpečeném operačním systému Alcatel-Lucent (AOS), který používá zabezpečený diverzifikovaný kód k ochraně sítí před potenciálními zranitelnostmi a útoky. Kód je průběžně aktualizován, aby řešil současné i budoucí hrozby. Softwarová diverzifikace prostřednictvím randomizace rozvržení adresního prostoru (ASLR) slouží k ochraně před útoky přetečení vyrovnávací paměti. Nezávislé ověření a validace (IV&V) se také používá k analýze a testování zdrojového kódu AOS z hlediska potenciálních zranitelností, zadních vrátek, malwaru a zneužití systému. Experti na kybernetickou bezpečnost třetích stran provádějí testy, které jsou prováděny na softwarových obrazech s obecnou dostupností, aby byla zajištěna integrita softwaru.

Používáme makro- a mikro-segmentaci, abychom zajistili přístup k síti s nulovou důvěrou. Obě jsou zásadní součásti strategie zabezpečení s nulovou důvěrou. **Makrosegmentace** odkazuje na rozdělení sítě do samostatných zón nebo domén na základě funkce, aplikace nebo skupiny uživatelů. Poskytuje vysokou úroveň segmentace sítě, což organizacím umožňuje izolovat důležité položky a zdroje od zbytku sítě. **Mikrosegmentace** se na druhé straně zaměřuje na segmentaci sítě na detailnější úrovni až na jednotlivého uživatele nebo zařízení. Tento přístup poskytuje detailnější kontrolu nad přístupem k síti a umožňuje organizacím prosazovat zásady zabezpečení na úrovni jednotlivých uživatelů nebo zařízení.

[Shortest Path Bridging \(SPB\)](#)

a **Universal Network Profiles**

(UNP) poskytují výkonné řešení, které pomáhá s makro- a mikro-segmentací sítí, což zlepšuje zabezpečení a výkon omezením rozsahu potenciálních útoků.

SPB je síťový protokol vrstvy 2, který umožňuje vícecestné směrování ve velkých sítích a zároveň zjednodušuje konfiguraci a správu síťové infrastruktury. Funkce, jako je segmentace virtuální sítě, poskytují zvýšenou ochranu před neoprávněným přístupem a kybernetickými útoky. Používáním protokolu SPB ve své síťové infrastruktuře mohou organizace těžit z lepší efektivity a zabezpečení sítě, což jim pomáhá s jistotou splnit své obchodní cíle.

ALE UNP je řízení přístupu založené na profilech, výkonná funkce přepínače Alcatel-Lucent Enterprise, která správcům sítě umožňuje vytvářet a spravovat uživatelské profily pro přístup k síti na základě identity, polohy a zařízení. Mohou implementovat centralizovanou správu síťových zásad, což zjednodušuje konfiguraci a vymáhání zásad. Implementací profilů ALE UNP mohou organizace zlepšit viditelnost sítě, zabezpečení a kontrolu a zároveň zlepšit výkon sítě, chránit prostředky a zkrátit prostoje.

SPB a UNP společně umožňují správcům sítě efektivně spravovat a zabezpečit síťovou infrastrukturu tak, aby bylo možné:

- důsledně uplatňovat zásady v celé síti,
- segmentovat a izolovat zařízení IoT od jiných zařízení,
- minimalizovat útočnou plochu sítě.

Přehled řešení

Budování nákladově efektivní sítě s nulovou důvěrou



Robustní ověření

ALE poskytuje robustní ověřování prostřednictvím nástroje Unified Policy Authentication Manager (UPAM).

Klíčovou součástí kybernetické bezpečnosti je ověřování, což je proces ověření identity uživatele, zařízení nebo systému. Zahrnuje potvrzení toho, že uživatel nebo zařízení je tím, kým tvrdí, že je, obvykle poskytnutím nějaké formy identifikace, jako je uživatelské jméno a heslo.

Řešení ALE podporuje řadu metod ověřování uživatelů.

- **802.1X**, síťový ověřovací protokol, umožňuje zařízením připojit se k zabezpečené síti zadáním přihlašovacích údajů, jako je uživatelské jméno a heslo. Když se zařízení pokusí připojit k síti pomocí protokolu 802.1X, je nejprve ověřeno, než mu bude povolen přístup k síti. V ideálním světě se zařízení ověřuje prostřednictvím protokolu 802.1x.

Ověření vygeneruje záznam, který lze sdílet s bránou firewall.

- Pokud zařízení nepodporuje protokol 802.1x, alternativou je ověřování **MAC adres**. MAC adresa je digitální identifikační karta pro každé zařízení v síti. Je jedinečná a identifikuje každé zařízení a umožňuje komunikaci mezi nimi, podobně jako jmenovka pro váš počítač nebo telefon.
- ALE podporuje **otisky prstů zařízení a systému**. Pokud není vrácen žádný profil s jiným ověřením 802.1X nebo MAC, pokusíme se ověřit otisky prstů. Snímání otisků prstů v počítačové bezpečnosti je proces shromažďování informací o zařízení nebo systému, jako je jeho operační systém, software a otevřené porty, za účelem jeho identifikace a kategorizace a posouzení potenciálních rizik a zranitelností. Lze jej také použít k mapování na profil zařízení registrovaný v databázi inventáře IoT.

- ALE také poskytuje výchozí nastavení „catch all“ (zachytit vše) v případě, že není profil vrácen. Toto výchozí pravidlo „catch-all“ může povolit omezený přístup nebo zcela odepřít přístup, pokud primární ověřování selže.

K provedení těchto různých typů ověřování potřebujete místo pro vytvoření a správu přihlašovacích údajů uživatelů a zařízení. Je vyžadován nástroj UPAM, který je součástí řešení ALE Unified Access. Poskytuje centralizované služby ověřování, autorizace a účetnictví (AAA) pro síť. Umožňuje správcům sítě vytvářet a spravovat uživatelské profily pro přístup k síti mimo jiné na základě identity a polohy. Nástroj UPAM lze konfigurovat a spravovat prostřednictvím systému [Alcatel-Lucent OmniVista® Network Management System](#), který umožňuje správcům sítě definovat a vymáhat zásady přístupu k síti.

Přehled řešení

Budování nákladově efektivní sítě s nulovou důvěrou



Reakce na incidenty

Rychlá reakce na síťové incidenty je klíčovým faktorem při minimalizaci poškození systémů a sítí a zkrácení prostojů způsobených bezpečnostními útoky, jako jsou útoky DDoS (Distributed Denial of Service).

Minimalizujte rizika, maximalizujte kvalitu prostředí (QoE) a zvyšte bezpečnost pomocí nástroje [Alcatel-Lucent OmniVista Network Advisor](#).

OmniVista Network Advisor je inteligentní a autonomní systém založený na umělé inteligenci, který poskytuje monitorování sítě v reálném čase, vydává upozornění, když nastanou problémy, a navrhuje řešení pro různé síťové a bezpečnostní záležitosti, včetně útoků DDoS. Průběžně provádí audit konfigurace a analýzu výkonu sítě, takže dokáže rychle identifikovat potenciální problémy, zmírnit je a optimalizovat síť s minimálním až žádným zásahem IT.

Partnerství a integrace

Důležitým aspektem ověřování je integrace s branami firewall. Například prostřednictvím integrace s řešením Fortinet je možné uživatele nebo

zařízení ověřené v sítích LAN a/nebo WLAN současně a jednoduše ověřit také v braně firewall Fortinet.

V případě integrace brány firewall Palo Alto Networks (PAN) příští generace je možné uživatele nebo zařízení ověřené v sítích LAN a/nebo WLAN současně a jednoduše ověřit také v braně firewall PAN.

Naše partnerství se společností [Versa Networks](#) umožňuje bezpečný přístup k důležitým zdrojům bez ohledu na umístění uživatelů, dat, aplikací nebo zařízení. To se hodí zejména pro podniky s regionálními kancelářemi nebo pobočkami, které jsou vzdálené od centrálního pracoviště nebo datového centra. Na rozdíl od tradičních sítí WAN, které vyžadují více síťových přeskoků a mohou způsobit dodatečné náklady, SASE a SD-WAN poskytují nákladově efektivní a bezpečné řešení pro éru od klienta do cloudu. Díky kombinaci těchto dvou řešení mohou firmy zjednodušit správu IT infrastruktury a umožnit bezpečný přístup k internetu a podnikovým aplikacím pro práci odkudkoli, včetně podniků/DC, regionálních kanceláří / poboček a domácích/mobilních pracovníků.

Tato [nabídka ALE-Versa Titan](#) je komplexní řešení, které kombinuje služby Secure Access Service Edge (SASE) a SD-WAN z cloudu. Zahrnuje službu Versa Titan SD-WAN, která poskytuje cloudovou SD-WAN pro štihlé IT, stejně jako službu Versa Secure Access (VSA), která obsahuje funkce brány firewall příští generace a geografické blokování, spolu se službou Zero Trust Network Access (ZTNA) pro práci odkudkoli. Versa Secure Web Gateway (SWG) také poskytuje bezpečné procházení webu a přístup k internetovým aplikacím (SaaS) pro bezpečné připojení vzdálené/domácí kanceláře. Webový portál a aplikace Versa Titan nabízejí integrované síťové a bezpečnostní služby na jediné platformě se všemi komponentami SASE poskytovanými stejným dodavatelem. Díky jedinému úložišti zásad, které zahrnuje zásady sítě a zabezpečení, mohou firmy zjednodušit správu IT a zajistit bezpečný přístup k důležitým zdrojům.

Přehled řešení

Budování nákladově efektivní sítě s nulovou důvěrou



Metodologie nulové důvěry

Aby organizace mohly implementovat model nulové důvěry, musí nejprve vyřešit problémy ve své stávající bezpečnostní infrastruktuře, jako jsou nekonzistentní zásady, implicitní důvěra a zranitelná zařízení IoT. Cílem je vytvořit přístup k síti a možnosti řízení přístupu na základě rolí, segmentace a monitorování, aby bylo možné s těmito problémy bojovat, se správnou segmentací, která umožňuje rozdělení citlivých zdrojů a omezení přístupu pouze na osoby, které jej potřebují. Funkce monitorování a karantény umožňují zákazníkům identifikovat a izolovat potenciální hrozby.

Jednoduchá, ale výkonná metodologie pro budování sítě s nulovou důvěrou pomocí řešení ALE zahrnuje několik fází.

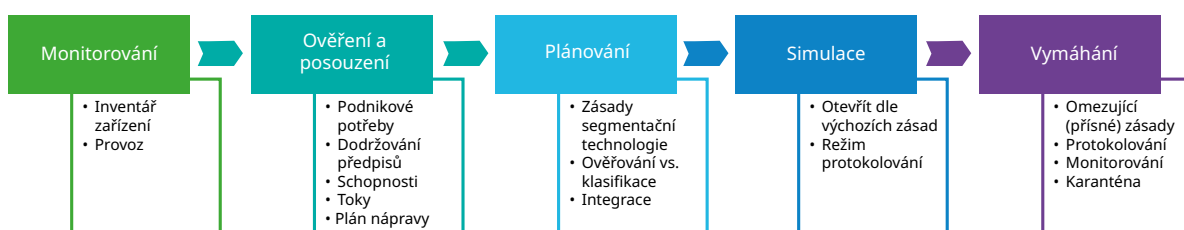
- **Monitorování:** Monitorování by mělo být prováděno včetně inventáře zařízení a provozu.
- **Ověření a posouzení:** Ověření a posouzení zahrnuje analýzu obchodních potřeb, požadavků na dodržování předpisů, možností a toků.
- **Plánování:** Na základě výsledků posouzení by měl být vytvořen plán opatření. Plánování zahrnuje výběr správné technologie a zásad segmentace a také zvažování ověřování vzhledem ke klasifikaci a integraci.
- **Simulace:** Ve fázi simulace jsou zásady ve výchozím nastavení otevřené a v režimu protokolování a budou testovány ostatní funkce.
- **Vymáhání:** Tato fáze vymáhání zahrnuje zavádění restriktivních zásad, protokolování, monitorování a provádění karanténních opatření.

Celkové náklady na vlastnictví

Celkové náklady na vlastnictví (TCO) pokrývají všechny náklady spojené s vlastnictvím a provozováním produktu nebo služby po celou dobu jejich životnosti. Patří mezi ně mimo jiné kupní cena, údržba, podpora a upgrady. Je důležité vybrat nákladově efektivní řešení, která nabízejí dlouhodobou hodnotu, což může snížit překročení rozpočtu a poskytnout přesnější návratnost investic (ROI).

Zvažte rozdíl mezi počáteční kapitálovou investicí a průběžnými výdaji potřebnými k zajištění licence na systém a udržení systému v provozu. Zatímco některé komponenty, jako jsou brány firewall, jsou zaměřeny čistě na zabezpečení, jiné komponenty jsou zásadní také pro vytvoření důkladnější strategie zabezpečení. Patří mezi ně správa zásad, efektivní technologie oddělení sítí cest (pokročilá a automatizovaná makro- a mikro-segmentace), automatické přiřazení virtuální sítě (VLAN), protokol šifrování sítě, viditelnost aplikací a nezávislé ověření a potvrzení kódu operačního systému.

Strategie kybernetické bezpečnosti sítě společnosti ALE řeší základní prvky zabezpečení sítě uvedené výše bez poplatků, zatímco alternativy od jiných dodavatelů vyžadují specifické odborné znalosti a řadu nákladných prvků a licencí pro provoz a údržbu. Metoda ALE poskytuje zákazníkům značné ekonomické výhody a zároveň zajišťuje silnou a efektivní kybernetickou bezpečnost sítě.



Přehled řešení

Budování nákladově efektivní sítě s nulovou důvěrou



Závěr

Je zřejmé, že implementace sítě s nulovou důvěrou pro robustní zabezpečení může přinést několik problémů, jako je složitost a náklady související s jejím vytvořením a údržbou. ALE však nabízí jedinečný a nákladově efektivní přístup k řešení těchto problémů. Pokročilé technologie makro- a mikro-segmentace spolu s dalšími komponentami uvedenými v tomto dokumentu poskytují jednoduchý a cenově dostupný způsob implementace sítě s nulovou důvěrou, která řeší moderní požadavky na kybernetickou bezpečnost. Jsme odhodláni pomáhat našim zákazníkům řešit jejich obavy ohledně kybernetické bezpečnosti a věříme, že náš přístup nám může pomoci tohoto cíle dosáhnout.

Řešení ALE zahrnují naši odolnou a bezpečnou službu [intelligentn Fabric \(iFab\)](#) a UNP a robustní řízení přístupu k síti (NAC) pomocí nástroje UPAM, který poskytuje řízení přístupu založené na profilech. Naše inovativní řešení [OmniVista Network Advisor](#) zajišťuje hladký provoz a rychlé zotavení a prevenci útoků. Kromě toho spolupracujeme s dodavateli SASE, jako je Versa Networks, a podporujeme integrace s dodavateli bran firewall, jako je Palo Alto Networks, abychom zákazníkům poskytli komplexnější a integrovanější bezpečnostní řešení.