



Architektura nulové důvěry

Co to je a jak jí dosáhnout



Obsah

Co je architektura nulové důvěry.....	3
Pochopení makro- a mikrosegmentace.....	5
Proč potřebujete obojí.....	6
Jak toho dosáhnout.....	7
Metodika.....	7
Ještě jedna věc.....	12
Proč ALE?.....	12
Co víme jistě.....	13



Co je architektura nulové důvěry?

Co znamená architektura nulové důvěry (zero trust architecture, ZTA)? Znamená to, že každý uživatel a zařízení musí být před povolením přístupu k datům ověřen a autorizován. Jde o strategii „nikomu nevěřit, vše ověřovat“.

Zde pomůže analogie.

Pokud uvažujeme o tradiční bezpečnosti jako o pevnosti, která chrání vesnici, postavili bychom okolo vesnice (jinak známé jako podnik) zeď pevnosti (jinak známou jako firewall). Všechno, co přichází zvenčí pevnosti, je nedůvěryhodné a podrobeno přezkoumání, ale cokoli uvnitř pevnosti je implicitně důvěryhodné a povoleno. Tato hranice důvěry je fyzická i implicitní, a to podle toho, na jaké straně pevnosti jste, protože pokud jste na „správné“ straně zdi, nejsou vyžadovány žádné další kontroly. Pokud uvažujeme o tomto přístupu z hlediska podnikové sítě, může existovat základní segmentace ve formě VLAN, SSID, podsítí nebo rozhraní vázaných na bránu firewall, ale tato segmentace je statická a má více společného se škálovatelností a ovladatelností sítě než se zabezpečením.

Dnes je však přístup brány firewall (pevnost) z mnoha důvodů sám o sobě méně účinný. Prvním důvodem je mobilita. Uživatelé se připojují k jiným sítím mimo podnik a mohou s sebou přinášet hrozby. Za druhé nemusí být hosté nutně důvěryhodní. Dalo by se tvrdit, že ani zaměstnanci (ti uvnitř pevnosti) by neměli být slepě považováni za důvěryhodné. A do třetice, do sítě je přidáváno stále více zařízení IoT. Představují vyšší bezpečnostní rizika, protože nemusí být sankcionována a řízena oddělením IT a obvykle jim chybí bezpečnostní funkce. Pokud při tradičním přístupu „pevnost/vesnice“ nebo „firewall/podnik“ dojde k narušení uživatele nebo zařízení, máloco zabrání tomu, aby se hrozba přelila na ostatní uživatele a zařízení. Jakmile jste jednou uvnitř, už vás nic neomezuje.

U analogii pevnosti se věc má tak, že pokud mezi vetřelci a vesnicí stojí pouze zeď, dojde v okamžiku, kdy se vetřelci naučí zeď překonat (a oni se to naučí), ke krveprolití.





Otázkou je, co s tím můžeme dělat. Přemýšlejme o tom z přístupu „nikomu nevěřit“, nebo „nulová důvěra“.

V případě nulové důvěry není důvěryhodný žádný uživatel ani zařízení. Ať už jsou v areálu nebo mimo prostory, procházejí stejnými kontrolami. Neexistuje nic jako důvěra vůči interním uživatelům. Každý přístup je ověřen a autorizován.

V analogii pevnosti by to znamenalo, že kromě pevnosti, která chrání vesnici před vnějšími hrozbami, má každý dům a každá budova své vlastní zabezpečení na ochranu před riziky majícími původ v nekalých aktérech, kteří žijí uvnitř pevnosti. V kontextu podniku to pak takzvaná softwarově definovaná mikrosegmentace posouvá o další krok dále. Kromě pevnosti a zabezpečení kolem budov máme také osobní stráž, které nás sledují na každém kroku. A ať se vydáme kamkoliv, budeme muset prokázat svoji totožnost. V podnikové síti je tato hranice důvěryhodnosti neostrá, distribuovaná a mobilní. Není vázána na konkrétní místo, port přepínače nebo VLAN. Záleží mimo jiné na identitě, zařízení, situaci a denní době. Je definována softwarově a upravována za povozu. V tomto přístupu musí být komponenty spravovány a měly by být schopny reagovat a podle potřeby být překonfigurovány tak, aby reagovaly na hrozby nebo změny v pracovním postupu.



Pochopení makro- a mikrosegmentace

V architektuře nulové důvěry existují dva druhy segmentace – makro- a mikrosegmentace. Pokud jde o naši analogii, stěna pevnosti je makrosegmentace a osobní bezpečnostní stráž je mikrosegmentace.

V **makrosegmentaci** je fyzická síť rozdělena do různých logických segmentů. Tyto segmenty mohou být VLAN, kombinace VLAN a VRF. Může to být také VPN, když mluvíme o přemostění nejkratší cestou (SPB), MPLS nebo dokonce VXLAN nebo tunelech GRE. Jakýkoli provoz mezi uživateli nebo zařízeními v různých segmentech je kontrolován bránou firewall. Všechny podniky používají nějak tvarovanou nebo formovanou segmentaci, ale ne vždy z bezpečnostních důvodů. Poměrně často se tento druh segmentace používá kvůli škálovatelnosti a z administrativních nebo organizačních důvodů. Pokud jsou dvě zařízení namapována na různé sítě VLAN, ale mohou komunikovat bez procházení bránou firewall, pak jsou ve stejném makrosegmentu. Typickým příkladem tohoto druhu segmentace je provozování IP telefonie na samostatných sítích VLAN a VRF, které jsou logicky izolovány od počítačů.

Otázkou je, jak do těchto segmentů namapujete uživatele nebo zařízení. I když to lze provést staticky, například přepínačem nebo SSID, jde to opravdu zastaralý způsob počínání. Je příliš nepružný a nevede si dobře s mobilními uživateli. V ideálním případě byste měli softwarově definovaný ověřovací systém, takže když se uživatel nebo zařízení připojí a dojde k jeho ověření, bude mu přiřazen profil. Profil zajistí uživateli nebo zařízení správný segment bez ohledu na fyzické umístění, port přepínače nebo SSID.

I když má makrosegmentace bezpečnostní výhody, v mnoha případech se realizuje z organizačních nebo administrativních důvodů. Například kamery a zámky dveří spadají pod kontrolu skupiny zabezpečení přístupu, zatímco termostaty spadají pod kontrolu skupiny údržby budov.

Mikrosegmentace posouvá věci o krok dále. Ne všichni uživatelé jsou stejní a ne všichni uživatelé mají oprávněnou potřebu přístupu ke všem zdrojům. Stejný profil, který mapuje uživatele do segmentu, obsahuje také sadu zásad, které přidávají jemně odstupňovanou kontrolu nad oprávněními uživatele/zařízení, která se liší pro různé role, jako je HR nebo Finance. Je to známo jako **přístup založený na rolích** a přímo souvisí se **zásadou nejmenších privilegií**. A tak platí, že i když jsou kamery a zámky dveří ve stejném segmentu, nemusí používat stejné zdroje. Kamera musí komunikovat s videorekordérem a zámek dveří se svým serverem. Není třeba, aby kamera komunikovala se zámek dveří, stejně jako není potřeba, aby zámek dveří komunikoval s jiným zámek dveří. Tato jemně odstupňovaná oprávnění jsou implementována prostřednictvím zásad, které jsou součástí profilu a dynamicky aplikovány na zařízení po ověření.

Mikrosegmentace musí být z několika důvodů definována softwarově. Uživatelé ani zařízení IoT nejsou statické, pohybují se, připojují se a odpojují, zásady proto nelze vázat na místo nebo port. Ve skutečnosti musí být konfigurace mikrosegmentace dynamické na základě kombinace více faktorů, včetně kromě jiného na totožnosti uživatele nebo zařízení, denní době a umístění.

Stručně řečeno, když je komunikace mezi různými segmenty řízena bránou firewall, jedná se o makrosegmentaci. Když je komunikace ve stejném segmentu řízena zásadami kontroly přístupu k síti (Network Access Control, NAC) přidruženými k roli zařízení nebo uživatele, jedná se o mikrosegmentaci.



Proč potřebujete obojí

Co se stane, pokud použijete pouze jeden typ segmentace?

Podívejme se na makrosegmentaci. Problém při použití pouze tohoto přístupu spočívá v tom, že brána firewall se stává úzkým místem, protože veškerý provoz musí kvůli ověřování a autorizaci projít bránou firewall. To může vést k problémům s výkonem. V distribuční vrstvě můžete nasadit více bran firewall, ale to může být docela nákladné a nemusí nutně zlepšit výkon, protože brány firewall nejsou stavěné na rychlost. Kromě toho nyní existuje několik bodů prosazování zásad a více míst, která udržují zásady aktuální, takže je správa těžkopádná.

Druhá možnost, využívající pouze mikrosegmentaci, je také problematická. Pokud se jediné vynucování zásad provádí prostřednictvím zásad NAC, budou tyto seznamy zásad velmi dlouhé a složité a můžete vyčerpat limity kapacity zařízení.

Pointa je, že je lepší mít mezi těmito dvěma formami segmentace rovnováhu. Bránu firewall nechte řídit veškerý provoz mezi různými segmenty (vertikální) a zásady NAC nechte řídit provoz v daném segmentu (příčný).

Kombinací těchto dvou přístupů můžete zvládat bezpečnostní hrozby, které se přelévají z jednoho segmentu zabezpečení do druhého, stejně jako ty, které se pohybují napříč stejným segmentem. Hmatatelněji řečeno, mikrosegmentace je to, co brání útočníkovi, kterému se podařilo narušit kameru, aby toto narušení využil jako výchozího bodu k narušení dalších zdrojů, jako je zámek dveří.

Cílem je ověřit každé připojení a přiřadit oprávnění každému uživateli nebo zařízení. To znamená použití segmentace k zabránění šíření hrozeb příčným pohybem a nepřetržité monitorování a karanténa jakéhokoli uživatele nebo zařízení, které se stane nevyhovujícím.





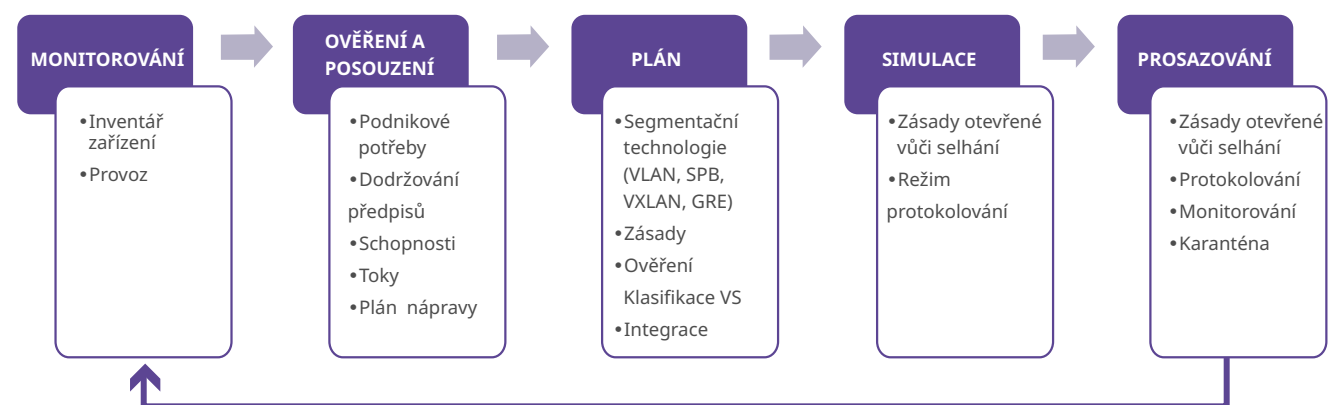
Jak toho dosáhnout

Kdybychom začínali od nuly, bylo by relativně snadné vybudovat architekturu s nulovou důvěrou pomocí mikrosegmentace od základů. Když ale od nuly nezačínáme, dovybavení sítě mikrosegmentací může mít za následek, že dojde k vyloučení uživatelů, zařízení a aplikací ze sítě kvůli neúspěšným ověřením nebo neúplným zásadám. Bylo by obtížné nebo dokonce nepravděpodobné, že by byl podnik schopen provést migraci najednou – v jediném modernizačním cyklu.

V prostředích se stávající strukturou bude existovat období, během kterého budou koexistovat nenulové architektury důvěryhodnosti a nulové důvěryhodnosti, a migrace nastane po jedné vrstvě nebo jednom místě najednou. Důležité je, abyste se ujistili, že nasazené prvky infrastruktury a způsob jejich nasazení jsou flexibilní a schopné pracovat v nulovém režimu důvěryhodnosti nebo v mikrosegmentovaném režimu, když jsou připraveny další prvky infrastruktury. To znamená, že infrastruktura bude muset spolupracovat se stávajícími a budoucími složkami.

Metodika

Existuje pět kroků směrem k architektuře s nulovou důvěrou - monitorování, ověření a posouzení, plánování, simulace a prosazování.



Obrázek 1 – Metodika



Krok 1: Monitorování

Než uděláte cokoli jiného, musíte začít sledovat a budovat mapu a inventář toho, co máte ve své síti.

Migrace na ZTA vyžaduje podrobnou znalost aktiv (fyzických a virtuálních), subjektů (včetně uživatelských oprávnění) a podnikových procesů, které se dotýkají nebo fungují v síti. Neúplné znalosti nejčastěji vedou k selhání tam, kde je přístup odepřen z důvodu nedostatečných informací. Jedná se zejména o problém, pokud v organizaci existují neznámé „stínové IT“ nebo „stínové IoT“.

Zahajte monitorování zařízení a provozních toků. Vytvořte zprávu o inventáři se všemi zařízeními, zobrazenými v síti, rozříděnými mimo jiné podle typu zařízení, výrobce, modelu a operačního systému. Zpráva by měla také ukázat, kde a který port přepínače nebo SSID zařízení naposledy viděl. Tyto informace lze získat z prvků, jako je adresa MAC, podpis DHCP a uživatelský agent HTTP.

Většina nástrojů třetích stran poskytne pouze IP adresu, nikoli typ zařízení. Bylo by ideální mít nástroj pro vytvoření inventáře IoT/zařízení, který usnadní rychlé a snadné vytváření profilů NAC pro jednotlivé typy zařízení.

Další informace potřebné pro vytváření zásad jsou provozní toky. V závislosti na vybavení, které máte, můžete tyto informace získat z nástrojů pro monitorování toku, jako jsou sFlow, Netflow nebo Deep Packet Inspection (DPI).

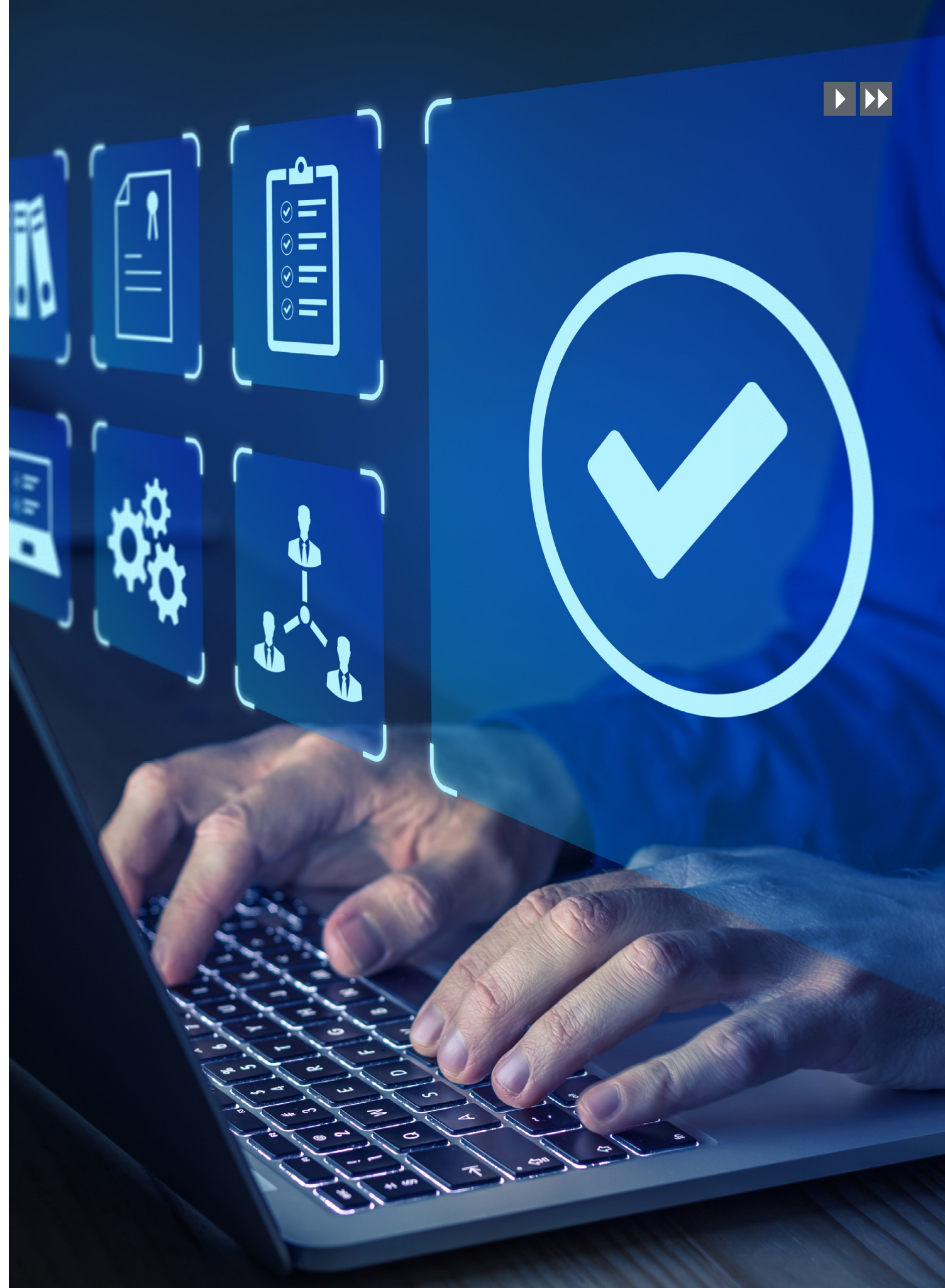
Tento proces bude iterativní. Když poprvé povolíte monitorování, zprávy nemusí být tak smysluplné, ale jak postupujete k dalším krokům, stanou se konkrétnějšími a užitečnějšími. Informace, které shromáždíte v tomto kroku, budou klíčové pro další kroky.



Krok 2: Ověření a posouzení

Dalším krokem je ověření těchto zjištění. Posuďte podnikové potřeby. Jakékoli stínové zařízení IoT, které nelze odůvodnit, by mělo být odstraněno, protože zbytečně zvětšuje prostor pro útok. Pokud jde o zbytek, musíte identifikovat subjekty (uživatelé a zařízení), provozní toky a pracovní postupy, protože budou muset být zohledněny ve vašich zásadách. Například kdo bude mít přístup ke konkrétním prostředkům a co s nimi bude moci dělat. Aplikujte zásadu nejmenších privilegií.

Mikrosegmentace neznamena uvolnění dalších bezpečnostních zásad, jako jsou zásady ohledně hesel nebo aktualizací firmwaru. Je třeba vyhodnotit jednotlivé schopnosti. Mohou tato zařízení podporovat ověřování založené na certifikátech? Existuje nástroj pro správu, který umožní vydávání a uplatnění těchto certifikátů? Jaké jsou požadovány provozní toky? Možná budete muset tyto informace získat od výrobce, ale měli byste je také porovnat s vlastními zprávami o analýze provozu. Pokud najdete prostředky, které nejsou v souladu se zásadami společnosti, potřebujete plán nápravy, který je uvede do souladu, nebo budete muset zavést další kontroly.





Krok 3: Plán

V této fázi již znáte prostředky, subjekty (uživatelé), provoz a pracovní postupy. Nyní je třeba tyto znalosti proměnit v zásady ověřování a zabezpečení, abyste mohli implementovat požadovanou architekturu mikrosegmentace. Jak již bylo zmíněno dříve, pro dosažení nejlepších výsledků byste měli zahrnout kombinaci makro- a mikrosegmentace. Mějte na paměti, že pokud nezačínáte budovat od nuly, budete většinou omezení architekturou, která je již zavedena.

Pro makrosegmentaci existuje několik možností, jako jsou VLAN, VRF, SPB VPN, VXLAN nebo tunely GRE a speciální funkce, jako je privátní VLAN. Všechny mají své výhody a nevýhody a mohou být v různých situacích užitečné. Pro mikrosegmentaci budete muset vědět, jaké zásady zahrnout do profilu pro jednotlivé typy uživatelů nebo zařízení. Nakonec budete muset definovat, jak mapovat uživatele a zařízení do jejich segmentu a zásad. To se týká autentizace nebo klasifikace, které mohou zahrnovat otisky prstů zařízení.

Ideálně byste měli investovat do technologie (softwarově definované segmentace), která vám umožní vytvářet flexibilní zásady ověřování, abyste mohli snadno aktualizovat síťové profily.

Autentizační tok doporučujeme navrhovat v tomto pořadí:

1. Ověřování pomocí certifikátů 802.1x s využitím serveru RADIUS. Ověřování generuje záznam o ověřování. Jedná se o informace, které lze sdílet s bránou firewall.
2. Pokud zařízení nelze ověřit pomocí certifikátů 802.1x, měli byste následně zkusit ověření MAC. Ověřování MAC není zdaleka tak bezpečné jako 802.1x, ale je lepší než vůbec žádné ověřování. Použijte jej, dokud nebudete připraveni postupovat k 802.1x.

3. Pokud není vrácen žádný profil, můžete zkusit otisky prstů, které můžete také použít k mapování segmentu profilu a pravidel. Tím se nevytvoří ověřovací nebo účetní záznam, ale zaznamená se do inventární databáze IoT.

4. Nakonec můžete nastavit výchozí „chytat všechno“ pro případ, že nedojde k vrácení profilů nebo pokud selže vše ostatní. V počátečních fázích budete stále muset mapovat zařízení na profil, který povede ke stejnému segmentu a pravidlům a bude zařízení zaznamenávat do databáze inventáře.

Tento tok by měl být strukturován flexibilním způsobem, abyste jej mohli průběžně vyladit. Možná například budete chtít nejprve odstranit ověřování MAC a přidat ho později, až budete mít seznam adres MAC získaných ze sestavy inventáře. A jak tento proces upřesníte, můžete například změnit segment a pravidla spojená s výchozím profilem na velmi omezující pravidla umožňující přístup pouze k hostiteli bašty.

Můžete také chtít sdílet roli zařízení s bránou firewall, aby pravidla brány firewall mohla být založena na roli zařízení, nikoli pouze na adrese podsítě/IP. Tato integrace má dvě výhody. Za prvé, brána firewall může na tato zařízení IoT aplikovat jemně odstupňované zásady. Za druhé, zásady brány firewall jsou nyní založeny na uživatelích nebo rolích, a proto již nejsou vázány na podsít' nebo IP adresu, což umožňuje budoucí změnu designu a opětovnou segmentaci sítě.

Proces bude iterativní a budete muset vyladit, naladit, a upřesnit, jak budete úspěšnější při používání ověřování a segmentace.



Krok 4: Simulace

Bez ohledu na to, jako moc plánujete, není pravděpodobné, že se to povede hned napoprvé. Jakákoli chyba v návrhu schématu ověřování, jakékoli opomenutí, které provedete v zásadě zabezpečení „seznam povolených“, bude mít za následek nefunkční podnikový proces. Budete muset použít zásady ověřování a přístupu v režimu „otevřeno vůči selhání“. To znamená, že zařízení a uživatelé, které se nepodaří ověřit, budou mít stále přístup do sítě a neočekávané přenosy budou nadále povoleny. Ale to vše bude zaznamenáno a pomocí těchto protokolů můžete upravit schémata ověřování a zásad.

Krok 5: Prosazování

Po jemném doladění již nebudete pozorovat selhání ověřování nebo odmítnutí legitimních toků. Tyto zásady pak můžete přesunout z režimu „otevřeno vůči selhání“ na „uzavřeno vůči selhání“, což znamená, že podloudná zařízení budou blokována a neočekávané toky budou zrušeny.

Je samozřejmé, že budete muset pokračovat v monitorování neočekávaných zařízení a dopravních toků – a celý cyklus podle potřeby opakovat.



Ještě jedna věc

V rámci průběžného monitorování, protokolování a karantény doporučujeme také investovat do externího systému detekce vniknutí (IDS). Přestože existuje řada útoků DDoS (Distributed Denial of Service), které lze identifikovat přímo samotným přepínačem, externí IDS může také detekovat širší škálu útoků, jako jsou viry nebo jiné anomálie. Možná si vzpomínáte, jak bylo před několika lety několik kamer infikováno malwarem Mirai, nebo na den, kdy tato zařízení zahájila koordinovaný útok na globální servery DNS, což ovlivnilo služby jako Twitter, Spotify nebo Paypal. Tyto útoky nemusí být detekovány vašimi přepínači, ale vyhrazená IDS je určitě zaznamenají.

Jakmile je útok detekován, IDS informuje váš systém správy sítě (NMS) o IP adresách dotčených zařízení. V ideálním případě by váš systém NMS měl být schopen tato zařízení vyhledat ve své databázi a změnit jejich profily na „karanténní roli“.

„Karanténní role“ je velmi omezující role, obvykle umožňující pouze komunikaci s hostitelem bašty, aby bylo možné zařízení napravit, například mimo jiné nastavením silného hesla nebo aktualizací jeho firmwaru.

Proč ALE?

Řešení [sítě digitálního věku](#) Alcatel-Lucent Enterprise Digital zahrnují robustní a flexibilní softwarově definovanou segmentaci s dynamickými zásadami DPI NAC, které umožňují postupný vývoj směrem k architektuře nulové důvěry.

Sít' digitálního věku je plán společnosti Alcatel-Lucent Enterprise, který umožňuje podnikům a organizacím vstoupit do digitální éry a rozvíjet své digitální podnikání. Je založen na třech pilířích:

- [Autonomní síť](#), která snadno, automaticky a bezpečně spojuje lidi, procesy, aplikace a objekty. Autonomní síť ALE je založena na efektivním portfoliu doplněném se skutečnou jednotnou platformou pro správu, která poskytuje společné bezpečnostní zásady napříč naší sítí LAN a WLAN. Autonomní síť také umožňuje flexibilní nasazení ve vnitřním, venkovním a průmyslovém prostředí. Správu sítě lze v závislosti na preferencích zákazníka poskytovat v místním prostředí, v cloudu nebo v hybridním nasazení.
- [Bezpečné a efektivní nasazení zařízení IoT](#): Díky segmentaci jsou zařízení izolována ve vyhrazených segmentech, což minimalizuje riziko ohrožení zabezpečení zařízení a sítě. Segmentace prvků IoT může podnikům pomoci snadno a automaticky zjistit, zda se zařízení chová správně či nikoli, a přispívá k zachování bezpečnosti sítě.
- [Podniková inovace](#) prostřednictvím automatizace pracovních postupů: Integrace metrik uživatelů, aplikací a IoT v reálném čase s geolokačními daty do platformy spolupráce zjednodušuje vytváření a zavádění nových automatizovaných digitálních obchodních procesů a služeb včetně oznámení správcům zabezpečení a sítě o případných narušeních, jakmile k nim dojde.

Máte nástroj pro vytvoření inventáře IoT/zařízení? Máte nástroj, který vám umožní sledovat toky aplikací? Jsou vaše aktuální přepínače a bezdrátové přístupové body připraveny pro softwarově definovanou segmentaci? Pokud tyto nástroje momentálně nemáte, [kontaktujte nás](#) a my vám s tím pomůžeme.



Co víme jistě

Na závěr uvedme několik klíčových poznatků:

- Chcete-li mít skutečně efektivní ZTA, musíte použít makro- i mikrosegmentaci
- Existuje pět kroků k ZTA: monitorování, ověření a posouzení, plánování, simulace a prosazování
- ZTA založené na mikrosegmentaci spočívá na třech pilířích: ověřování se zlatým standardem 802.1x EAP-TLS; diferencovaných zásadách spojených s rolí uživatele nebo zařízení, které sahají zpět k principu nejmenších privilegií; a na nepřetržitém monitorování a karanténě
- V hybridním a mobilním prostředí musí být mikrosegmentace definována softwarem, což znamená, musí být dynamická a založená na zásadách, nikoli staticky definovaná, jinak by to bylo nepraktické.

Migrace na ZTA prostřednictvím mikrosegmentace je proces. Je nepravděpodobné, že by ji podnik jakékoli významné velikosti zvládl během jediného modernizačního cyklu. Ale v každém cyklu modernizace nebo přepracování nebo neustálého zlepšování se můžete přiblížit tomuto cíli, pokud na místě zavedete správnou infrastrukturu a design.

Společnost Alcatel-Lucent Enterprise se zavázala vyvíjet síťové technologie a řešení, jež organizacím pomáhají realizovat jejich podnikatelský potenciál prostřednictvím digitální transformace.

