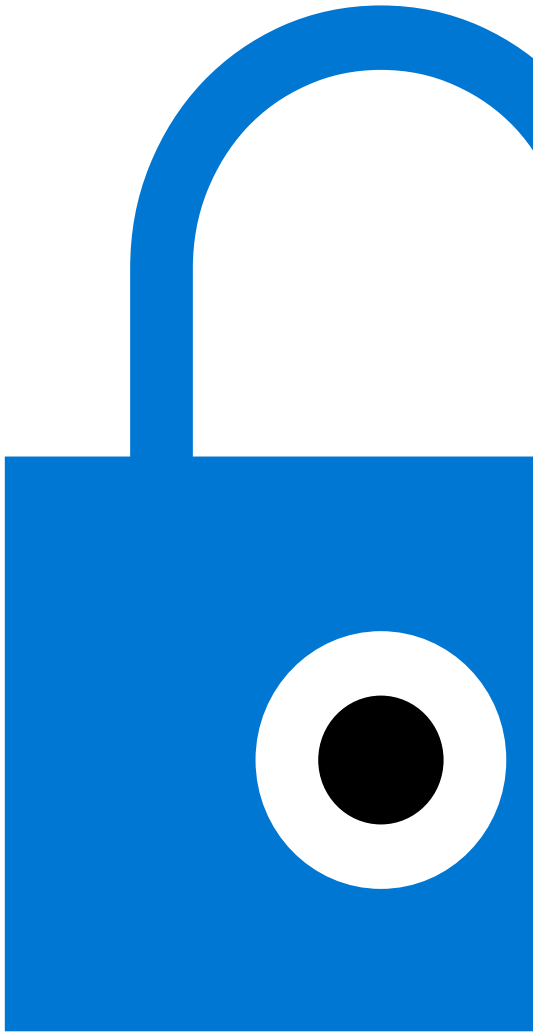
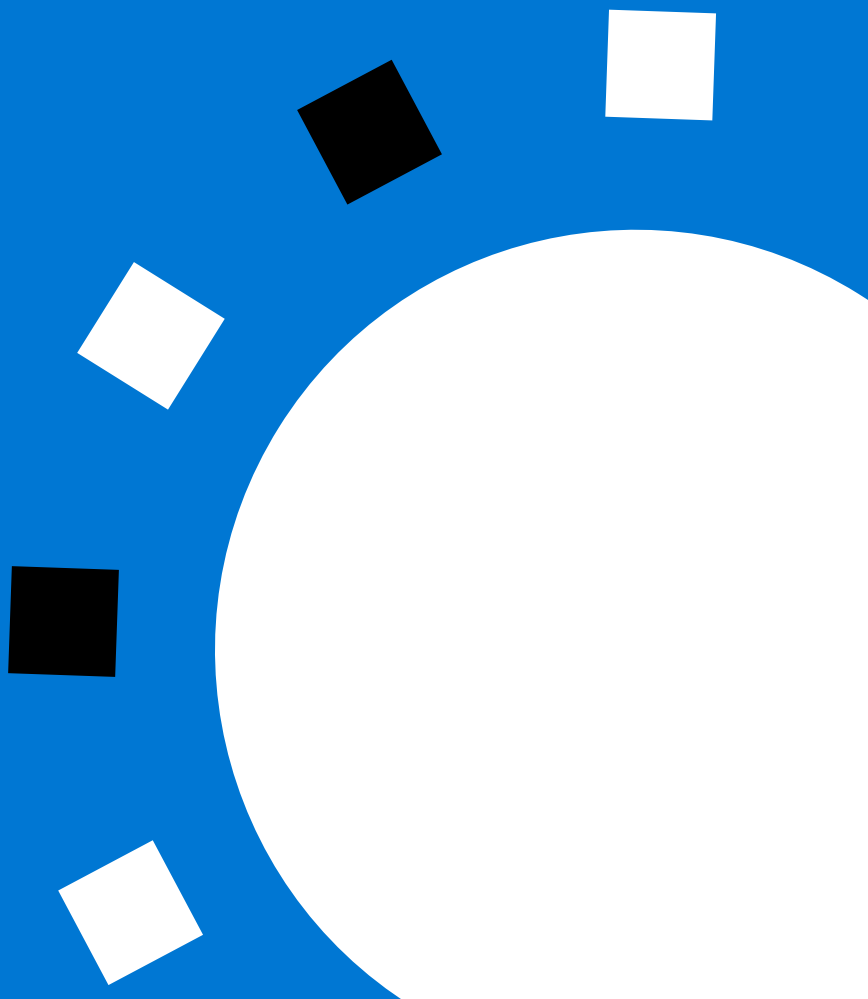
Microsoft



Zkoumání nulové důvěry (Zero Trust)

Kulatý stůl pro vedoucí pracovníky

Kulatý stůl



1. prosince 2020 uspořádala společnost Microsoft a organizace Cloud Security Alliance (CSA) virtuální kulatý stůl pro vedoucí pracovníky, jehož cílem bylo vést dialog zaměřený na problémy reálného světa a rozšířit vizi zabezpečení typu nulová důvěra. Kulatý stůl, kterého se zúčastnilo 10 vedoucích pracovníků z oblasti zabezpečení z významných energetických, finančních, pojišťovacích a výrobních společností, vedla Ann Johnson, viceprezidentka společnosti Microsoft pro rozvoj podnikání v oblasti zabezpečení, dodržování předpisů a identit. Tito vedoucí pracovníci sdíleli svoje poznatky a zkušenosti získané na cestě k nulové důvěře.

Hlavní poznatky

U kulatého stolu vedoucí pracovníci diskutovali o významu informační bezpečnosti pro digitální transformaci. Sdíleli svoje zkušenosti a konkrétní příklady budování strategického přístupu k informační bezpečnosti a diskutovali o přijetí základních principů nulové důvěry, které pomáhají zlepši celkovou úroveň informační bezpečnosti.

V tomto kontextu se účastníci zaměřili na následující témata:

- Odklon od zaměření na zabezpečení perimetru a přechod na holistický přístup k zabezpečení
- Zahájení cesty k přijetí nulové důvěry v menším měřítku a následné budování jednotlivých aspektů informační bezpečnosti
- Jak zlepšit přijetí zabezpečení typu nulová důvěra v rámci celé organizace

Strategie nulové důvěry pro moderní zabezpečení

Zabezpečení typu nulová důvěra není produkt ani řešení.

Jedná se o širší strategii pro moderní zabezpečení, která umožňuje efektivnější adaptaci na současné komplexní prostředí, je přívětivá pro mobilní pracovníky a chrání všechny osoby, zařízení, aplikace a data, ať už se nacházejí kdekoli. Na rozdíl od tradičních přístupů, které se pokoušejí vynutit to, aby všechny prostředky byly v „zabezpečené a kompatibilní" síti, se nulová důvěra zaměřuje na zabezpečení a dodržování předpisů u prostředků bez ohledu na jejich fyzické nebo síťové umístění.

To nahrazuje přesvědčení, že vše, co je na vnitřní straně podnikového firewallu, je bezpečné – naopak se předpokládá, že prolomení zabezpečení představuje reálnou hrozbu, a každý požadavek se proto ověřuje, jako by pocházel z nekontrolované sítě. Nulová důvěra nám velí „nikdy nedůvěřovat, vždy ověřovat", a to bez ohledu na to, odkud požadavek přichází nebo ke kterým prostředkům přistupuje.

Strategie nulové důvěry musí především zajistit základní principy a ochranu před hrozbami a následně přináší i další výhody, jako je zjednodušení.

Základní výhody	
Lepší ochrana před porušením zabezpečení	32 %
Rychlejší detekce hrozeb a náprava	30 %
Lepší ochrana dat zákazníků	29 %

Zdroj: Microsoft Zero Trust Survey 2020

K ochraně před porušením zabezpečení se používá všechno – od identit uživatelů až po hostitelské prostředí aplikací. Mikrosegmentace a zásady nejnižší možné úrovně oprávnění se používají k minimalizaci taktiky lateral movement a bohaté analytické nástroje a analýzy pomáhají získat lepší přehled, řídit detekci hrozeb a zlepšit obranu tím, že identifikují, co se stalo, co bylo ohroženo a jak zabránit opakování.

Prvky podporující přijetí nulové důvěry

Architektura na bázi nulové důvěry vyžaduje implementaci kontrolních mechanismů a technologií napříč všemi základními prvky: identitami, zařízeními, aplikacemi, daty, infrastrukturou a sítěmi. Každý z těchto prvků je zdrojem signálu, řídicí rovinou pro vynucování a důležitým prostředkem, který je třeba chránit. Proto je každý z nich také důležitou oblastí, na kterou je třeba zaměřit investice.

Identity jsou novým perimetrem

Z rozhovorů u kulatého stolu vyplynulo zásadní zjištění: Organizace se musí nejprve zaměřit na posílení ověřování uživatelů a identit, protože většina porušení zabezpečení zahrnuje krádež přihlašovacích údajů.

Vzhledem k tomu, že nedostatky v kybernetické hygieně zvyšují riziko pro jednotlivé zaměstnance i celou organizaci, je komplexní správa identit zásadní pro zajištění toho, aby k podnikovým datům měli přístup jenom oprávnění uživatelé.

Identity jsou novým perimetrem

Řízení přístupu pomocí identit

Identity – představující uživatele, služby a zařízení IoT – jsou společným jmenovatelem napříč sítěmi, koncovými body a aplikacemi. V modelu zabezpečení typu nulová důvěra fungují jako výkonný, flexibilní a podrobný způsob řízení přístupu k datům. Když se jakákoli identita pokusí o přístup k libovolnému prostředku, měl by proces správy provést následující akce:

- Ověřit identitu pomocí silného ověřování
- Zajistit, aby přístup splňoval příslušné požadavky a byl pro danou identitu typický
- Potvrdit, že identita dodržuje principy přístupu s nejnižší možnou úrovní oprávnění

Jeden z účastníků zdůraznil, že díky silné správě identit a přístupu došlo k následujícímu: „Už nespoléháme na perimetr. Novým perimetrem je identita a vy potřebujete silnou identitu, která jeověřená....Odtud tento projekt začal. Protože nemůžete dělat správu přístupu ručně, musí to být automatizovaný proces. Měli byste mít dobrou automatizaci a dobré přihlašovací údaje, aby vám všechno fungovalo tak, jak má.“

Identity jsou novým perimetrem

Používejte lepší ověřování

Můžete podstatně zlepšit stav zabezpečení informací ve své organizaci jednoduše tím, že do strategie správy identit zařadíte vícefaktorové ověřování (MFA) nebo průběžné ověřování. Jeden z účastníků kulatého stolu zdůraznil sílu tohoto přístupu a uvedl, že díky rozšíření správy identit o průběžné ověřovací profily může jejich organizace teď ověřovat identitu i v případě, že se změní IP adresa nebo běžný vzorec chování uživatele.

V souvislosti s nastavením identit pro operační technologie v terénu byl jeden z účastníků dotázán, která identita je důležitější: lidé, nebo počítače? Odpověděl: „Obojí. Potřebujete lidi, hlavně techniky, aby vyrazili do terénu a mohli využívat vícefaktorové ověřování. V minulosti to bylo obtížné, ale teď je to mnohem jednodušší. Největší problém pak spočívá v ověřování mezi počítači. Jak získáte druhý faktor, když nemáte člověka, který by ho mohl ověřit?“

Identity jsou novým perimetrem

Využívejte ověřování bez hesla

S rozvojem nulové důvěry se v rámci moderního přístupu k zabezpečení informací stále častěji používají biometrické údaje a další inovace. Další forma vícefaktorového ověřování, ověřování bez hesla, nahrazuje tradiční hesla bezpečnou alternativou. Tento typ ověřování vyžaduje dva nebo více ověřovacích faktorů zabezpečených pomocí páru kryptografických klíčů. Při registraci zařízení vytvoří veřejný a privátní klíč. Privátní klíč se dá odemknout jenom pomocí místního gesta, jako je PIN kód nebo biometrické ověření. Uživatelé se mohou přihlásit přímo pomocí biometrického rozpoznávání – například skenem otisku prstu, rozpoznáním obličeje nebo oční duhovky – nebo pomocí PIN kódu, který uzamčený a zabezpečený v zařízení.

Když byl jeden z účastníků dotázán na dopad ověřování bez hesla na efektivitu nulové důvěry, odpověděl: „Myslím, že ji zvyšuje. Po roce testování konceptu Microsoft Windows Hello ho teď zavádíme v celé organizaci. Nulová důvěra bude fungovat jenom v případě, že bude transparentní pro koncového uživatele. Musíte to udělat tak, aby to bylo snadné a transparentní. Pokud chcete provádět ověřování každých pět minut nebo každou sekundu, je to v pořádku, pokud koncový uživatel nemusí dělat nic – pokud to můžete ověřit jinými metodami. Koncový bod může být například jedním z faktorů vícefaktorového ověřování.“

Segmentace podnikové sítě

Segmentace sítě byla během rozhovorů u kulatého stolu předmětem intenzivní diskuse. Jeden z účastníků vyslovil názor, že když máte hodně segmentace, začne se všechno rozpadat. Když začnete navrhovat různé části a segmentovat hraniční síť, nebudete už mít plochou síť IT. To je pro firemní IT problém, protože brány firewall představují včasnou segmentaci, což má za následek potíže s vývojem a testováním. V konečném důsledku se IT tým stává více závislý na bezpečnostních týmech při řešení problémů se sítěmi, připojením a přístupem.

Ve světě mobilních a cloudových technologií jsou ovšem všechna důležitá firemní data dostupná prostřednictvím síťové infrastruktury. Síťové ovládací prvky poskytují důležité funkce, které vám umožní mít lepší přehled a pomáhají zabránit realizaci taktiky lateral movement v síti. To znamená, že organizace by měly pokračovat v segmentaci sítí a provádět hlubší mikrosegmentaci sítě a kromě toho také nasadit ochranu proti hrozbám v reálném čase, koncové šifrování, monitorování a analýzu.

Jeden účastník poznamenal: „Začali jsme mikrosegmentací a makrosegmentací naší sítě. Začali jsme v datových centrech a kancelářích, což vedlo k segmentaci aplikací s možností omezit uživatele na daný systém aplikací, když přicházejí přes VDI nebo VPN. Můžeme tedy segmentovat uživatele tak, aby po přechodu do naší sítě VPN nezískali neomezený přístup.“

V další diskusi o segmentaci byli účastníci dotázáni, jestli je možné architekturu na bázi nulové důvěry rozšířit i na místní prostředky, nebo jestli je lepší ji použít jenom pro cloudová prostředí. V reakci na tento dotaz se jeden z účastníků podělil o následující zkušenosti: „My jsme začali od místního prostředí a tak to bude i nadále, protože to potřebujeme k mikrosegmentaci pro ochranu před taktikou lateral movement atd. Tyto věci se nemění, pouze je teď rozšiřujeme do cloudu. U finančních služeb nikdy nebudeme mít všechno v cloudu, vždy budeme mít kombinaci místních a cloudových řešení....Budeme muset přijít na to, jak se postarat o všechny různé perimetry a jak rozšířit paradigma napříč všemi oblastmi."

Další účastník uvedl: „Začal jsem s větší mikrosegmentací a NAC. Opravdu jsem nedůvěřoval další síti VLAN. Museli jste přejít přes bránu firewall, pokud jste nebyli ověření, nemohli jste se tam dostat. Teď jsme se museli ujistit, že je možné procházet ze segmentu do segmentu a že je možné procházet obousměrně, jednosměrně. Tady to opravdu začalo."

Zabezpečení zařízení

Většina se shodne na tom, že moderní organizace se musí vypořádat s neuvěřitelnou rozmanitostí koncových bodů přistupujících k datům. Jeden z účastníků kulatého stolu ovšem vyjádřil obavu, že samotná zařízení jsou do značné míry ignorována. Ne všechny koncové body spravuje nebo dokonce vlastní organizace, což vede k různým konfiguracím zařízení a úrovním oprav softwaru. Jak už bylo zmíněno dříve, nulová důvěra se řídí zásadou „nikdy nedůvěřovat, vždy ověřovat". Z hlediska koncových bodů to znamená vždy ověřovat všechny koncové body – tedy nejen včetně zařízení dodavatelů, partnerů a hostů, ale také aplikací a zařízení, která zaměstnanci používají pro přístup k pracovním datům, bez ohledu na vlastnictví zařízení.

U modelu nulové důvěry se používají stejné zásady zabezpečení bez ohledu na to, jestli je zařízení vlastněné společností, nebo v osobním vlastnictví a jestli je zařízení plně spravované IT oddělením, nebo jsou zabezpečené jenom aplikace a data. Zásady se vztahují na všechny koncové body – PC, Mac, smartphone, tablet, nositelné zařízení nebo zařízení IoT – bez ohledu na to, kde jsou připojené – ať jde o zabezpečenou firemní síť, domácí širokopásmové připojení, nebo veřejný internet.

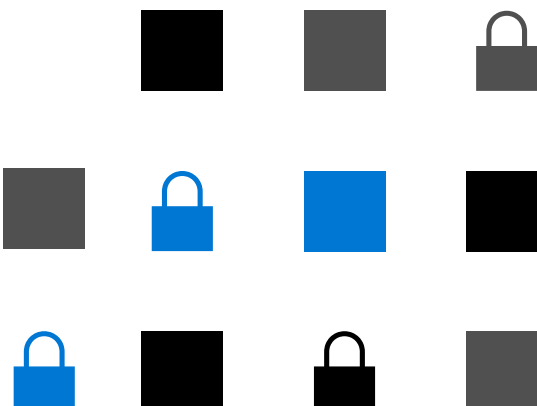
V rozhovoru o zařízení jeden z účastníků uvedl obzvláště přesvědčivý příklad: „Ve světě, kde si uživatelé přinášejí vlastní zařízení (BYOD), je zařízení velmi výbušnou součástí. Pokud umožníte, aby se k vaší síti připojovala nespravovaná zařízení, je to, jako kdyby se někdo dostal do vaší základny s živou municí, a může to rychle způsobit problémy. Proč byste tedy pro začátek netestovali venku? Lidé si časem zvyknou, že jsou vyzýváni k tomu, aby si věci zabezpečili (například zajistili opravy zařízení), a bude se to od nich očekávat. Uživatelé se naučí očekávat tato připomenutí a zabezpečovat zařízení."

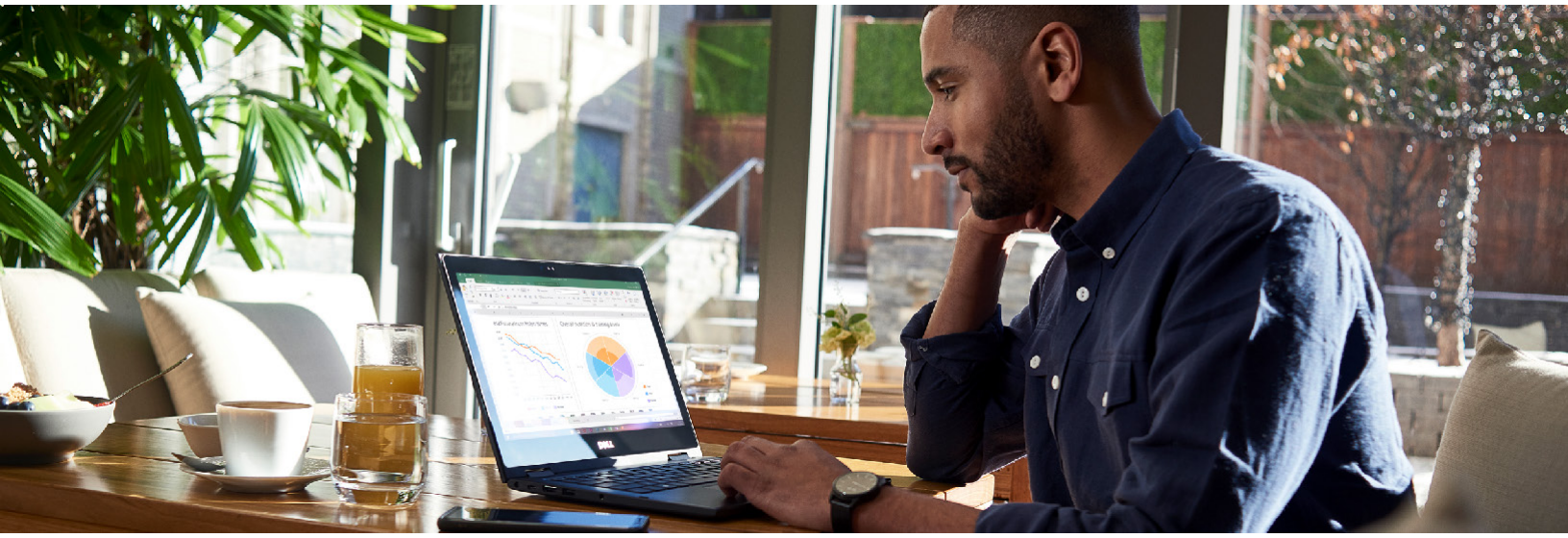
Segmentace aplikací

Za zvláštní zmínku stojí, že někteří účastníci kulatého stolu vyjadřovali svoje obavy týkající se zabezpečení na úrovni aplikací. Zdůrazňovali, že pro úspěšnou implementaci strategie nulové důvěry hraje zásadní roli správně nastavený přístup k aplikacím, ať už prostřednictvím SaaS, nebo v datových centrech.

Aby organizace mohly plně využívat všechny výhody cloudových aplikací a služeb, musí najít správnou rovnováhu mezi poskytováním přístupu a zachováním kontroly, aby byla zajištěna ochrana aplikací a dat, která obsahují. Měly by se používat kontrolní mechanismy a technologie ke zjišťování stínového IT, zajištění vhodných oprávnění v aplikaci, přístupu k bráně na základě analýz v reálném čase, monitorování neobvyklého chování, omezení akcí uživatelů a ověřování možností zabezpečené konfigurace.

Při diskusi o cestě k nulové důvěře se jeden z účastníků podělil o své myšlenky týkající se zabezpečení aplikací: „Je stále snazší a dosažitelnější mít segmentaci mezi aplikacemi. Možnost poskytovat zvýšená oprávnění nebo přístup na základě role se stává součástí modulu zásad. Zdá se, že součást týkající se aplikací se řeší postupem času stále inteligentněji. Tento přístup se ověří pokaždé, když uslyším, že se koncový uživatel může vyřešit daný problém.“



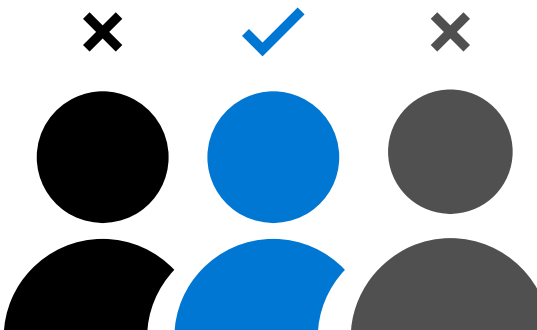


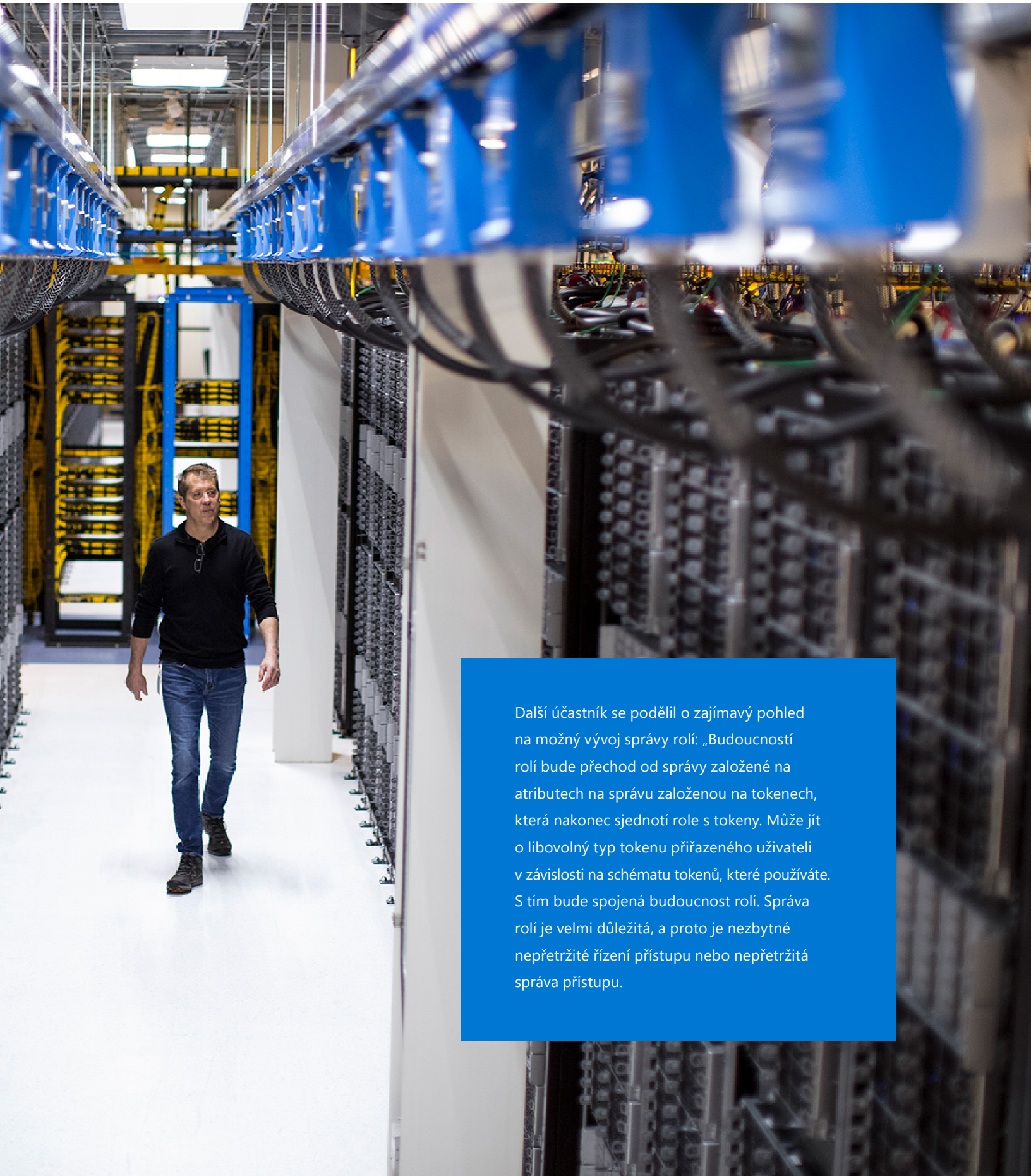
Definování rolí a řízení přístupu

Při řešení nejnaléhavějších otázek dneška účastníci rozhovorů u kulatého stolu věnovali čas rychlému rozšíření práce na dálku. Většina zaměstnanců teď pracuje na dálku a organizace musí zvážit alternativní způsoby, jak zavádět moderní kontrolní mechanismy zabezpečení. Jeden z účastníků se přímo zaměřil na operace a uvedl, že správa uživatelských rolí pomocí zásad je klíčovou součástí systému zabezpečení informací. Tato myšlenka byla následně rozšířena o nutnost efektivní správy rolí – a propojení rolí se zásadami jako součást ověřování, jednotného přihlašování (SSO), přístupu bez hesla, segmentace atd.

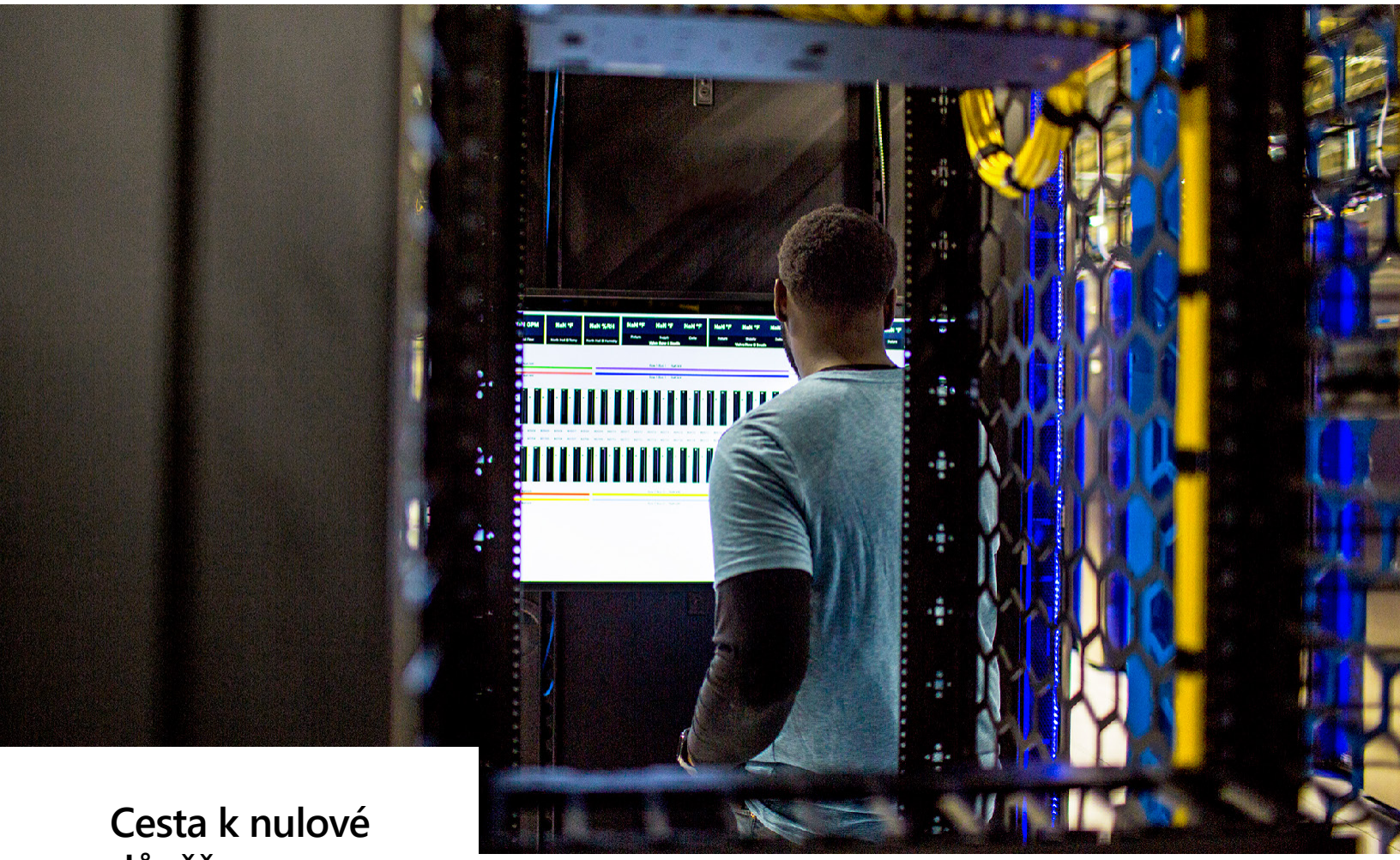
Zbývá tedy zodpovědět tuto otázku: Jak efektivní je spravovat role na úrovni operací a propojit je se správou zásad? Podle jednoho účastníka je ve skutečnosti nezbytné operacionalizovat role – aby totiž bylo možné povolit jednotné přihlašování a funkce bez hesla, je třeba definovat správné role. Tento účastník ovšem také doporučoval opatrnost a varoval před příliš velkým počtem rolí. Každá definovaná role se musí spravovat teď i v budoucnu, což může způsobit rozrůstání a rizika, protože role mohou zůstat nemonitorované nebo mít více oprávnění, než je potřeba.

Při debatě o efektivním definování rolí jeden z účastníků uvedl: „Chcete mít velmi podrobné nastavení ověřování, ale když nakonec vytvoříte v organizaci tisíc rolí, které budou takto podrobné, budete mít problémy s průběžnou správou. Nakonec budete mít obrovské množství účtů, které jsou neaktualizované a to je situace, kdy dochází k porušením zabezpečení – jako když se přesunu do jiné části organizace a vezmu si tato oprávnění (která už nepotřebuji) s sebou do nové role."





Další účastník se podělil o zajímavý pohled na možný vývoj správy rolí: „Budoucností rolí bude přechod od správy založené na atributech na správu založenou na tokenech, která nakonec sjednotí role s tokeny. Může jít o libovolný typ tokenu přiřazeného uživateli v závislosti na schématu tokenů, které používáte. S tím bude spojená budoucnost rolí. Správa rolí je velmi důležitá, a proto je nezbytné nepřetržité řízení přístupu nebo nepřetržitá správa přístupu.



Cesta k nulové důvěře

Když účastníci kulatého stolu diskutovali o svých zkušenostech s nulovou důvěrou – jak začínali a kde se v současné době nacházejí, objevilo se několik společných motivů. Hlavním problémem byla nutnost porozumět rozsahu zabezpečení informací a identifikovat výchozí bod. Někteří účastníci začínali svou cestu k nulové důvěře správou identit a přístupu uživatelů, jiní začali s makrosegmentací a mikrosegmentací sítě a další uvažovali z hlediska aplikací. Nakonec všichni přešli na vyspělý model nulové důvěry tím, že nedůvěřují nikomu ani něčemu jinému – uvnitř ani vně zdi, na koncových bodech, na serveru, v cloudu atd. Shodli se na tom, že s tím, jak se nulová důvěra vyvíjí, se vyvíjí i uvědomění, že neexistuje žádný cíl a že všechno je jenom cesta.

Jeden z účastníků uvedl, že svou cestu k zabezpečení na bázi nulové důvěry zahájili správou identit. Chtěli implementovat funkce jednotného přihlašování a uvědomili si, že je možné je rozšířit i na práci z domova.

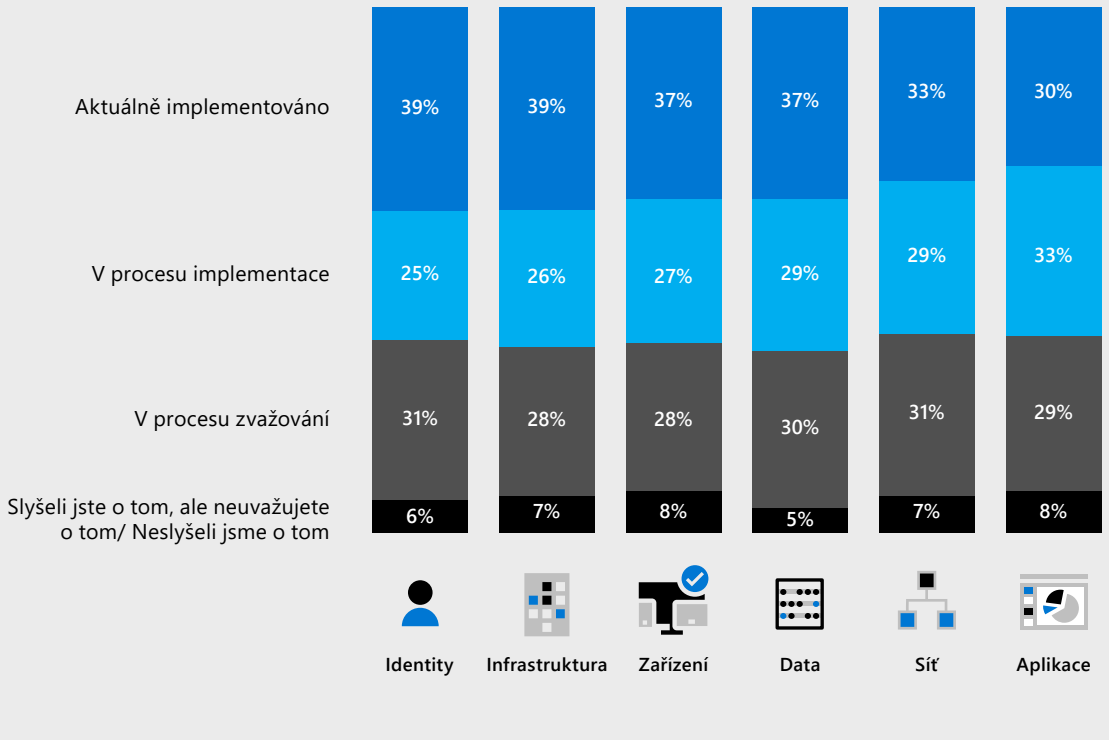
Pro řešení nulové důvěry je velmi důležité vypracovat ucelenou strategii. Pokud chce organizace definovat a realizovat úspěšnou cestu k nulové důvěře, musí zvážit priority podniku, technologie, procesy a dokonce i dopad změn.

Účastníci kulatého stolu se shodli, že:

Je třeba začít v malém, vybudovat si důvěru a poté zavést nulovou důvěru v celé organizaci, aby byla zajištěna optimální ochrana.

Nulová důvěra je komplexní strategie s implementací napříč všemi pilíři

Aktuální stav aktivit souvisejících s nulovou důvěrou
Celkem (n=300)



Zdroj: Microsoft Zero Trust Survey 2020

Začněte v malém a budujte důvěru

Požadavky organizace, stávající technologie a fáze zabezpečení – to vše ovlivňuje plánování implementace nulové důvěry. Přestože je zabezpečení na bázi nulové důvěry nejefektivnější při integraci napříč všemi digitálními prostředky, mnoho organizací bude muset zvolit postupný přístup, který bude cílit na konkrétní oblasti na základě vyspělosti jejich modelu nulové důvěry, dostupných prostředků a priorit. Každá investice se musí pečlivě zvážit a sladit s aktuálními potřebami firmy. Prvním krokem na této cestě nemusí být rozsáhlá změna ani přechod na cloudové nástroje zabezpečení.

Když chcete začít s nulovou důvěrou, nemusíte ani úplně přebudovat infrastrukturu. Nejúspěšnější řešení by měla být vrstvou nad hybridním prostředím a měla by ho podporovat, aniž by zcela nahradila stávající investice.

Bez ohledu na velikost organizace by se při nasazování nulové důvěry mělo začít od malých částí, protože dělat několik větších změn současně často není proveditelné. Úspěchu se obvykle dosáhne tím, že začnete s úplně novým projektem v cloudu nebo experimentujete ve vývojovém a testovacím prostředí.

Jeden z účastníků zdůraznil svůj názor na to, že je třeba začít v malém, slovy: „Musíte začít od nejcennějších prostředků, ale nepokoušejte se dělat všechno. Pokoušet se nasadit nulovou důvěru a zároveň dělat několik dalších věcí není možné.“

Jiný účastník se podělil o zkušenost z reálného života, kdy se mu podařilo přesvědčit velkou organizaci, aby s nulovou důvěrou začala v malém: „Udělal jsem workshop s velkou bankou a řekl jsem jim, že by měli začít v malém. Jejich odpověď zněla: „Začneme v malém s 5 000.“ Z jejich úhlu pohledu to bylo malé, ale já jsem jim odpověděl: „Začněte s 50.“ Banka nesouhlasila a začala s asi 2 500. Asi za osm týdnů banka přišla zpět a chtěla přehodnotit rozsah a to, jak má pilotní plán vypadat. Banka začala znovu s 25 osobami. Teď už jsou to dva roky a postupují dál.“

Rozšíření na celý systém

Po provedení prvních kroků a získání důvěry by se měl model nulové důvěry rozšířit na veškeré digitální prostředky a zároveň sloužit jako integrovaná filozofie a komplexní strategie zabezpečení. Pokud se strategie nulové důvěry použije na celý systém, musí pokrýt kompletní stav zabezpečení.

Vyhodnocení připravenosti na model nulové důvěry

Organizace, které začínají vyhodnocovat svou připravenost na model nulové důvěry a plánovat vylepšenou ochranu napříč svými digitálními prostředky, by měly zvážit následující klíčové investice, které pomohou zajistit bezproblémovou a efektivní implementaci nulové důvěry.

Silné ověřování: Jako základ každé strategie přístupu zajistěte silné vícefaktorové ověřování a detekci rizik relací, aby se minimalizovalo riziko ohrožení identit.

Adaptivní přístup založený na zásadách: Definujte přijatelné zásady přístupu pro prostředky a vynucujte je pomocí konzistentního modulu zásad zabezpečení, který poskytuje zásady správného řízení i přehled o odchylkách.

Mikrosegmentace: Přejděte od jednoduchého centralizovaného síťového perimetru ke komplexní a distribuované segmentaci pomocí softwarově definovaných mikroperimetrů.

Automatizace: Investujte do automatizovaného upozorňování a nápravy, aby se zkrátila průměrná doba reakce na útoky.

Analýza a umělá inteligence: Využívejte cloudovou analýzu a všechny dostupné signály k detekci a reakci na anomálie v přístupu v reálném čase.

Klasifikace a ochrana dat: Zjišťujte, klasifikujte, chraňte a monitorujte citlivá data, abyste minimalizovali riziko jejich zneužití nebo náhodné exfiltrace.

Zdroj: Microsoft Zero Trust Maturity Model (model vyspělosti nulové důvěry)

Každá žádost o přístup by měla být před udělením přístupu důkladně zkontrolována, jestli neobsahuje anomálie. Vše od identity uživatele až po hostitelské prostředí aplikace by mělo být ověřeno a autorizováno pomocí mikrosegmentace a zásad přístupu s nejmenší možnou úrovní oprávnění, aby se minimalizoval prostor pro taktiku lateral movement.

Stručně řečeno, aby organizace implementovaly model zabezpečení typu nulová důvěra konzistentně a komplexně, měly by zvážit všechny základní prvky, včetně identit, zařízení, aplikací, dat, infrastruktury a sítě. Kromě toho by se měly zohlednit následující aspekty:

- Všechny uživatele a zařízení pokoušející se získat přístup k prostředkům je třeba ověřit z hlediska důvěryhodnosti pro přístup k cílovému prostředku (na základě citlivosti cílového prostředku).
- Za účelem konzistentního uplatňování zásad organizace na všechny prostředky by se měl používat jediný modul zásad nulové důvěry (a ne několik modulů, jejichž konfigurace by se mohla lišit).
- Čím více měření odrážejících běžné chování je zahrnuto do rozhodnutí o důvěryhodnosti, tím obtížnější a nákladnější je pro útočníky napodobit legitimní pokusy o přihlášení a činnosti, což útočníky odrazuje nebo omezuje jejich možnosti způsobit škody.
- Systémové operace by měly vždy zůstat v bezpečném stavu, a to i po neúspěšném nebo nesprávném rozhodnutí (například zachování životnosti/bezpečnosti a obchodní hodnoty prostřednictvím zajištění důvěrnosti, integrity a dostupnosti).
- Udržování v bezpečném stavu je zvlášť důležité pro organizace spoléhající na starší nebo statické ovládací prvky, které nemohou dynamicky měřit a vynucovat důvěryhodnost příchozích pokusů o přístup (například statické síťové ovládací prvky pro starší verze aplikací, serverů nebo zařízení).

Jeden z účastníků se podělil o zkušenosti své organizace s postupnou cestou k vyspělému modelu nulové důvěry:

„Začali jsme základní cestou ručního provádění mikrosegmentace (před vytvořením SDP) a potom jsme implementovali NAC. Potom se spolu se zavedením IoT a cloudu a ztenčením hranice interních a externích perimetrů rozvíjely další aspekty nulové důvěry – například segmentace aplikací, segmentace sítě, federace identit, průběžné ověřování a vícefaktorové ověřování – a rozrostlo se to do plnohodnotného ekosystému."

Největší motivací k přijetí strategie nulové důvěry je zlepšení celkového stavu zabezpečení a potom také to, že bezpečnostní hrozby se neustále vyvíjejí.

Motivace k zavedení modelu nulové důvěry
Celkem (n=300)

Zdroj: Microsoft Zero Trust Survey 2020

Nikdy nedůvěřujte, vždy ověřujte

Model zabezpečení na bázi nulové důvěry vytváří efektivní kontrolní mechanismy pro důležité firemní informace a systémy a zajišťuje tak správným lidem přístup ke správným datům ve správný čas. Na základě principu „nikdy nedůvěřovat, vždy ověřovat“ nulová důvěra pomáhá zabezpečit firemní prostředky tím, že eliminuje neznámá a nespravovaná zařízení a minimalizuje možnost uplatňovat taktiku lateral movement. Vzhledem k tomu, že nulová důvěra poskytuje komplexní strategii napříč celým systémem, včetně identit, infrastruktury, zařízení, dat, aplikací a sítě, implementace skutečného modelu nulové důvěry vyžaduje, aby všechny tyto prvky byly ověřené a označené jako důvěryhodné.

I když cesta k modelu nulové důvěry může být obtížná, je to základní prvek jakéhokoli dlouhodobého plánu modernizace. Každá organizace, která chce přijmout nulovou důvěru, by měla začít tím, že použije kontrolní mechanismy zabezpečení na malých částech – není třeba se pokoušet vynucovat více větších kontrolních mechanismů současně. Jakmile budou kontrolní mechanismy zabezpečení úspěšně používány v rámci postupného přístupu, může být zabezpečení na bázi nulové důvěry rozšířeno napříč všemi digitálními prostředky. Ideální prostředí nulové důvěry zahrnuje silné ověřování identit, zařízení zaregistrovaná ve správě zařízení, uživatelská práva s nejnižšími možnými oprávněními a ověřený stav služby.

Další informace

Objevte zabezpečení typu nulová důvěra

Vyhodnoťte, kde se v rámci cesty k nulové důvěře nacházíte

Centrum Microsoftu pro nasazení nulové důvěry