CSO

Microsoft Security

SPONZOROVANÝ OBSAH

Zabezpečení Zero Trust (nulová důvěra): **Zkušenosti prvních uživatelů**

CSO Microsoft Security

Obsah

- Úvod
- Zero Trust je tady a přináší hodnotu
- Hnací síly zavádění Zero Trust
- O hrozby není nouze
- Překážky pro zavedení Zero Trust
- Výzvy spojené s nasazením
- Osvědčené postupy pro nasazení Zero Trust
- V jaké fáze nasazení modelu Zero Trust se nacházíte?

CSO Microsoft Security

Úvod

Poslední dva roky chaosu otřásly tradičními modely IT a zabezpečení. Díky tomu se zabezpečení Zero Trust (nulová důvěra) rychle změnilo ze zajímavého konceptu na základ moderního podnikového zabezpečení.

Nový průzkum společnosti Foundry zjistil, že 52 % organizací zkouší nebo nasadilo architekturu Zero Trust a dalších 15 % zkoumá modely Zero Trust. Tito uživatelé uvádějí řadu výhod, které plynou z nasazení, včetně lepší ochrany dat zákazníků, snížení složitosti či zajištění bezpečného a spolehlivého přístupu k podnikovým zdrojům.

V této e-knize se seznámíte s výsledky výzkumu společnosti Foundry. Tyto výsledky zdůrazňují význam strategie Zero Trust (nulové důvěry), která pomáhá vedoucím pracovníkům CISO chránit jejich organizace před řadou riziky z mnoha vektorů útoků. Obsahuje také návod, jak zavést koncept Zero Trust pro ty, kteří s ním teprve začínají.

O průzkumu

Společnost Foundry provedla v únoru a březnu 2022 průzkum mezi americkými podniky, aby zjistila aktuální stav zavádění modelu Zero Trust (nulová důvěra). Respondenti museli být vedoucími IT oddělení nebo vyššími pracovníky ve společnosti s více než 500 zaměstnanci a podílet se na nákupu produktů a služeb kybernetického zabezpečení.

Celkem 250 respondentů se zapojilo do průzkumu, který obsahoval 23 otázek.

CSO Microsoft Security

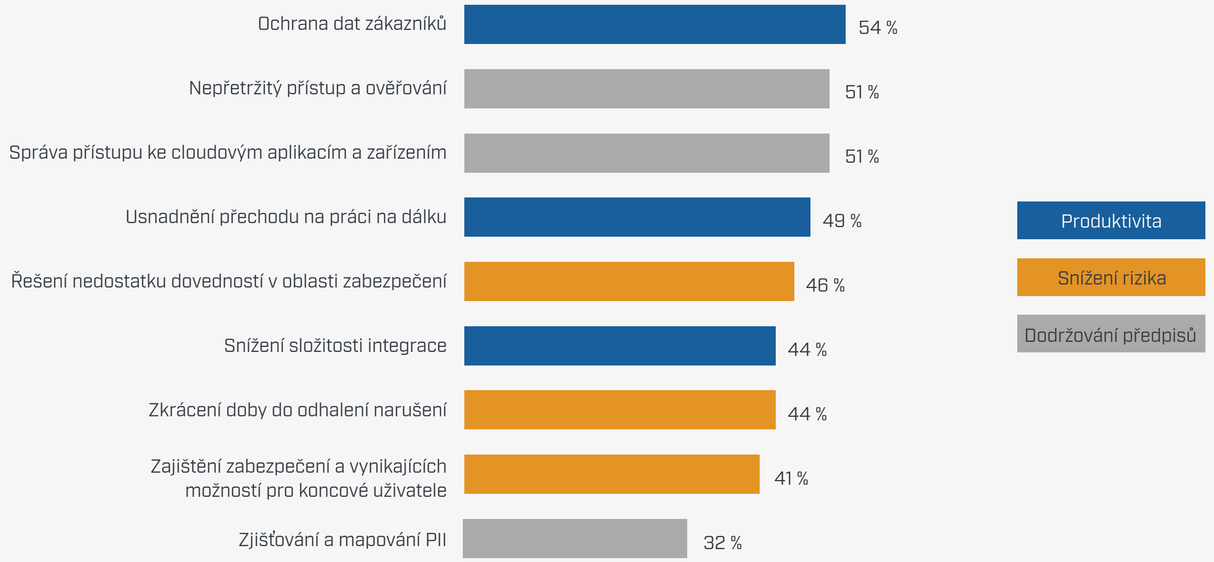
Zero Trust je tady a přináší hodnotu

Z výsledků průzkumu a hloubkových rozhovorů s vedoucími pracovníky v oblasti IT a zabezpečení je zřejmé, že ve většině organizací je přístup Zero Trust na prvním místě. A společnosti, které nasadily různé komponenty Zero Trust, již vidí jejich výhody.

Většina respondentů, kteří implementovali model Zero Trust (87 %), tvrdí, že tato architektura splňuje nebo překračuje jejich původní cíle v oblasti implementace, přijetí a integrace.

„Metoda [Zero Trust] se pro nás stala standardním operačním postupem. Nedokážu si představit, že bychom se někdy vrátili k tomu, co jsme dělali předtím," říká ředitel IT globálního maloobchodního řetězce. (Respondentům byla poskytnuta anonymita výměnou za to, že mohli svobodně hovořit o svých plánech v oblasti zabezpečení.)

Přínosy získané zavedením modelu Zero Trust



12 % respondentů uvedlo, že dosahuje *všech* těchto výhod

Zdroj: Zero Trust Adoption Survey, březen 2022, Foundry. Základ: 250

CSO Microsoft Security

Přibližně 44 % respondentů také uvedlo, že model Zero Trust snižuje složitost spojenou s implementací integrované architektury zabezpečení. „Vzhledem k tomu, že se zabýváte a pracujete s architekturou, je to méně komplikované," říká CISO společnosti s call centrem o 3 500 zaměstnancích.

Viceprezident a CISO ve firmě poskytující finanční služby se 17 000 zaměstnanci tvrdí, že vícefaktorové ověřování, které jeho společnost zavedla v rámci modelu Zero Trust, se zaměstnancům líbí. „Ve skutečnosti to zvýšilo spokojenost zaměstnanců, protože nyní nemusejí používat firemní počítač a klienta VPN, ale mohou se ke zdrojům dostat odkudkoli," říká.

Koncept nejméně privilegovaného přístupu se rovněž vyplatil, poznamenává CISO. „Díky zavedení tohoto systému přístupu k oprávněním jsme zaznamenali méně katastrofálních chyb správců systému," říká. „Oprávnění získávají pro konkrétní záležitosti a v konkrétních časových rámcích, díky čemuž je méně pravděpodobné, že udělají chybu."

Vzhledem k rostoucímu výskytu phishingu a dalších kybernetických útoků shrnuje ředitel IT v maloobchodní společnosti výhody Zero Trust takto: „Kdybychom neměli tyto typy nástrojů, pravděpodobně bychom se právě teď ocitli ve špatné situaci a platili někomu bitcoiny."

CSO Microsoft Security

Hnací síly zavádění Zero Trust

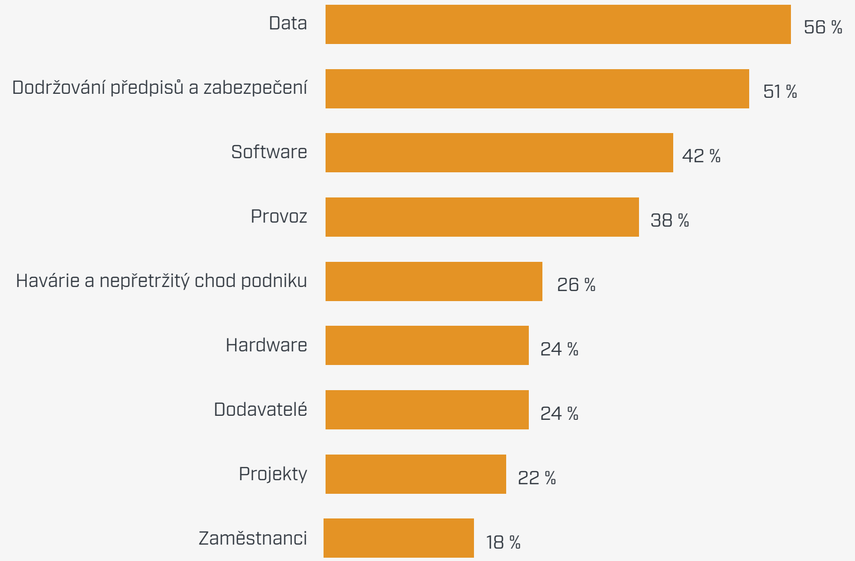
Souběh událostí vede společnosti k tomu, aby architekturu Zero Trust přinejmenším zvážily. Na prvním místě seznamu je potřeba zvládat rizika pro množství prostředků proti četným hrozbám. Respondenti průzkumu přičítali několikaleté incidenty v oblasti zabezpečení řadě příčin, v čele s ohrožením zabezpečení od osob nebo organizací třetích stran. Další důvody zahrnovaly:

- Neočekávaná obchodní rizika
- Chybná konfigurace služeb nebo systémů
- Zlomyslné a úmyslné útoky zevnitř
- Nezáměrné chyby uživatelů, včetně obětí phishingu
- Ohrožené identity
- Neopravený software
- Ukradené přihlašovací údaje

Tyto incidenty představují různá rizika, především v oblasti dat.

V mnoha organizacích urychlil náhlý přechod na práci na dálku, který byl způsoben pandemií, plány na zavedení modelu Zero Trust. Tradiční modely zabezpečení založené na perimetru totiž zastaraly. Mnoho organizací se tímto směrem vydalo již dříve, protože přesouvaly více aplikací a IT infrastruktury do cloudu, ale pandemie se stala dalším impulsem.

Hlavní kategorie ohrožené hrozbami v oblasti kybernetického zabezpečení



Zdroj: Zero Trust Adoption Survey, březen 2022, Foundry. Základ: 250

CSO Microsoft Security

Například CISO společnosti zabývající se zdravotnickými technologiemi o 1 700 zaměstnancích říká, že cloud a pandemie se staly hnacím motorem pro zavedení modelu Zero Trust, který nyní poskytuje bezpečný základ pro jakýkoli budoucí model pracoviště.

„Obchodní důvody spočívaly v tom, že jsme cloudová společnost a potřebovali jsme zabezpečit naše prostředí," říká. „Během pandemie jsme také museli zajistit schopné pracovníky na dálku. [Zero Trust] nám umožnil dramaticky snížit náš rozsah nemovitostí a pravděpodobně zůstaneme minimálně z 60 % virtuální vzdálenou společností."

CSO Microsoft Security

O hrozby není nouze

Podnětem pro robustnější modely zabezpečení jsou také požadavky na dodržování předpisů. „Regulační orgány nás sledují a očekávají, že budeme pokračovat ve zlepšování našeho rámce zabezpečení," říká viceprezident pro globální zabezpečení informací ve společnosti, která poskytuje finanční služby a využívá více než 290 000 zaměstnanců.

Některé organizace aktivně podnikly kroky k dosažení modelu Zero Trust, aby se vyhnuly závažnému narušení, které by je dostalo do centra pozornosti z nesprávných důvodů. „Šlo o to být proaktivní a snažit se nedostat se do zpráv," říká CIO z instituce vyššího vzdělávání s 3 500 zaměstnanci. „Slyšel jsem skutečné hororové příběhy z jiných místních institucí přibližně naší velikosti, které nefungovaly dlouhou dobu."

Jiné již zažily vážný incident týkající se kybernetického zabezpečení, což je přimělo rychle přehodnotit svou strategii v oblasti zabezpečení. Poté, co pojišťovna s 6 000 zaměstnanci zažila útok ransomwaru, který na dva týdny odstavil firemní síť, přišel mandát k zavedení modelu Zero Trust přímo od CEO. „Implementaci jsme urychlili," říká viceprezident firmy pro vývoj IT. „Na začátku to byly určitě osvědčené postupy a po útoku ransomwaru se to velmi zrychlilo."

Katalyzátor v podobě cloudu

Viceprezident a CISO významné společnosti poskytující finanční služby říká, že jeho tým si uvědomil potřebu nové architektury zabezpečení již před několika lety, když začal využívat více cloudových prostředků a uživatelé se stali mobilnějšími.

„Uvědomili jsme si, že tradiční architektura zabezpečení typu „hrad a příkop", na kterou jsme se spoléhali v minulosti, nás před útočníky v budoucnu neochrání," říká.

Tato skutečnost se stala zcela zřejmou na začátku roku 2020, kdy společnost zjistila, že někdy v předchozím roce pronikl útočník přes její perimetr a pohyboval se v prostředí, aniž by byl detekován. „Potřebovali jsme novou architekturu, která by umožnila chránit a ověřovat používání těchto prostředků bez ohledu na to, kde se nacházejí. Architektura Zero Trust je k tomu určena."

CSO Microsoft Security

Překážky pro zavedení Zero Trust

Pro mnoho organizací představuje Zero Trust (nulová důvěra) zásadní změnu ve struktuře zabezpečení, procesech a způsobu myšlení. To vysvětluje některé překážky, které musí před zavedením tohoto modelu překonat.

„V rámci organizace existovalo tolik různých sil, že jsme narazili," poznamenal CISO call centra a vysvětlil, že týmy zabývající se servery, sítěmi a databází měly každý svůj vlastní kontingent webových serverů a nástrojů. „To nás brzdilo, protože každý měl jinou představu o tom, kam se vydat a jak to udělat."

Co brání zavedení modelu Zero Trust?

Zdroj: Zero Trust Adoption Survey, březen 2022, Foundry. Základ: 250

CSO Microsoft Security

Anthony Mocny, vedoucího marketingového manažera produktu pro model Zero Trust ve společnosti Microsoft, tvrdí, že odhalení takových problémů může být ve skutečnosti pozitivním vedlejším efektem modelu Zero Trust. „Jako architektura je Zero Trust navržena tak, aby rozbila sila bezpečnostních týmů, které fungují v rámci jednotlivých technologických pilířů, a pomohla týmům pracovat společně a jednotně," říká. „Může to znamenat i kulturní změnu, pokud jde o způsob spolupráce týmů."

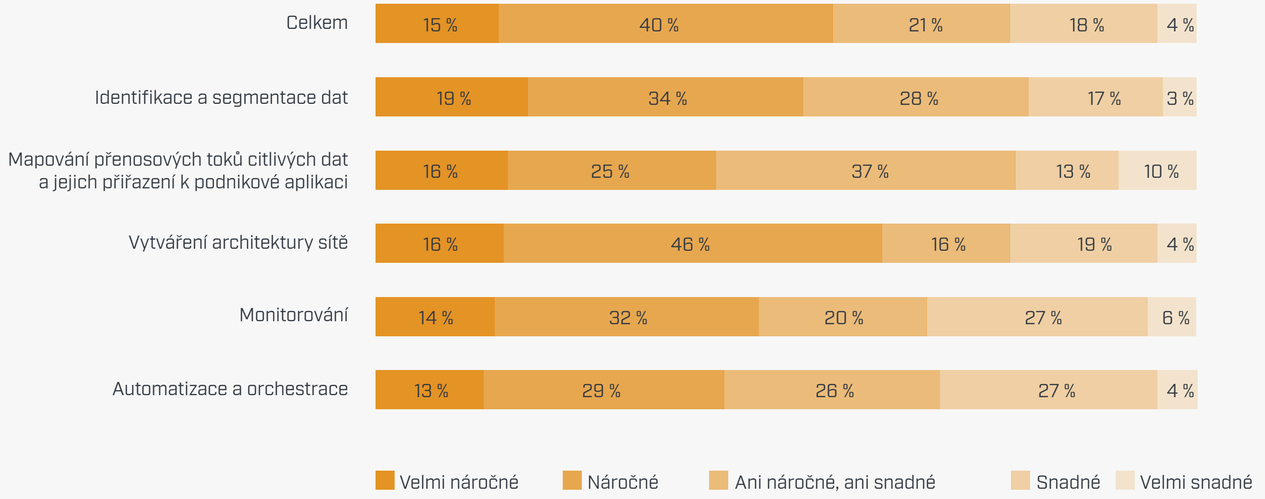
Pro viceprezidenta/CISO finančních služeb byly starší aplikace překážkou, kterou bylo třeba překonat na cestě k architektuře Zero Trust. „Musí být modernizovány pomocí moderní technologie ověřování," říká. „V závislosti na jejich stáří to nemusí být úplně snadné."

CSO Microsoft Security

Výzvy spojené s nasazením

Jakmile se společnosti vydají na cestu Zero Trust, mohou se objevit různé problémy při implementaci. Více než polovina respondentů průzkumu (56 %) připustila, že zavedení architektury Zero Trust je náročné nebo velmi náročné. Konkrétně:

Jak náročná je implementace Zero Trust?



Zdroj: Zero Trust Adoption Survey, březen 2022, Foundry. Základ: 168

CSO Microsoft Security

V hloubkových rozhovorech se často objevovaly problémy, které se týkají segmentace a mikrosegmentace.

„Segmentujete síť až na jednotlivé hostitele," říká viceprezident/CISO pro finanční služby. „Je to jako postavit malý firewall mezi všechny hostitele ve vnitřní síti, abyste viděli veškerý provoz a mohli ho kontrolovat až k jednotlivým počítačům. To má obrovské výhody z hlediska zabezpečení, ale je velmi obtížné to implementovat, protože musíte v podstatě spravovat desítky tisíc firewallů."

Mapování provozních toků může být další proces, který trvá několik měsíců. CTO vydavatelské a mediální společnosti s 5 000 zaměstnanci po definování kritických dat, aplikací a síťových služeb, které potřebují chránit, „zmapoval transakční toky v síti a snažil se je chápat jako skupiny informací," říká. „[Poté jsme] segmentovali části těchto informací a způsob, jakým skutečně procházejí sítí, a to až na jednotlivé pakety informací." V tomto bodě společnost aplikovala zásady Zero Trust na každý typ datového toku. „Vybudovali jsme také nové možnosti monitorování a údržby naší sítě."

Navzdory problémům se mnoho respondentů domnívá, že architektura Zero Trust v konečném důsledku zjednodušuje každodenní provoz. S tradičními technologiemi „trvá několik dní, než provedete změny – musíte je rozeslat po všech hardwarových a softwarových komponentách, a na to spotřebováváme spoustu prostředků," říká viceprezident pro globální zabezpečení informací ve finančních službách. „Když se podíváme na Zero Trust, skutečně z dlouhodobého hlediska minimalizuje složitost architektury a snižuje počet zaměstnanců, které potřebujeme pro stejný typ práce."

Osvědčené postupy pro nasazení Zero Trust

S přibývajícím počtem společností, které zavádějí architekturu Zero Trust, vznikají plány a osvědčené postupy, které mohou ostatní následovat. Níže uvádíme pět bodů, které je třeba zohlednit při plánování nasazení.

Na začátku to nepřehánějte

Mapování strategie modelu Zero Trust může být náročné, pokud se na ni díváte pouze v širokém kontextu nutnosti revize zásad a ochrany napříč sítěmi, daty, aplikacemi, identitami, koncovými body a infrastrukturou. „Na začátku to byl jen pohled na obrovskou horu, kterou jsme museli zdolat. Pochybovali jsme, zda to opravdu zvládneme," říká CIO v oblasti vyššího vzdělávání. „Musíte na to jít postupně."

CIO a jeho tým nakonec přijali přístup „peníze až na prvním místě" a upřednostnili segmentaci finančních a mzdových aplikací v samostatné síti.

Identifikace nejkritičtějších aktiv, která je třeba chránit, je podle Mocneho správný přístup. „Mějte na paměti, proč vůbec zavádíte architekturu Zero Trust", říká.

Když jste na pochybách, začněte s vícefaktorovým ověřováním

Při určování priorit souboru řešení zabezpečení doporučuje řada CISO i dodavatelů, abyste se nejprve zaměřili na ověřování a další ochrany založené na identitě. „Pokud ještě nemáte vymyšlený výchozí bod, představuje vícefaktorové ověřování ideální začátek," říká Mocny. Microsoft odhaduje, že vícefaktorové ověřování může zabránit více než 90 % útoků založených na identitě.

Viceprezident/CISO v odvětví finančních služeb souhlasí. „Ověřování představuje základní prvek implementace architektury Zero Trust. Žádná z ostatních komponent nemůže fungovat, pokud nelze ověřit totožnost koncového uživatele, takže jsme začali právě tam."

Následně se viceprezident/CISO v odvětví finančních služeb zabýval síťovou komponentou, která přinesla okamžité výhody pro podporu vzdálených pracovníků. Tým ponechal mikrosegmentaci až na pozdější fázi cesty, protože není dobře viditelná pro celou firmu. „Po dokončení podstatně zvýšíte zabezpečení, ale nikdo nepozná rozdíl," říká.

CSO Microsoft Security

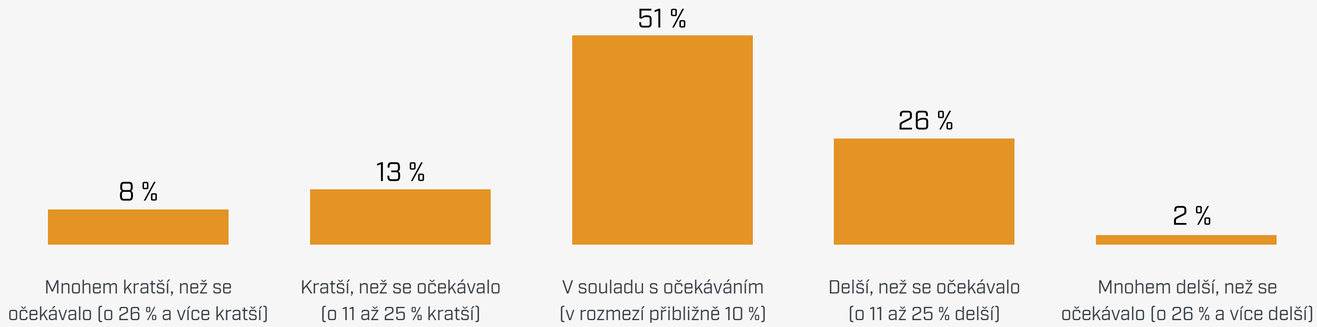
Zůstaňte realističtí ohledně časových plánů

Je důležité, aby CISO stanovili realistická očekávání ohledně nasazení architektury Zero Trust. „Zavedení architektury Zero Trust je program, nikoli projekt," říká viceprezident/CISO v odvětví finančních služeb. „To byla obrovská změna. Správná implementace zahrnuje řadu projektů a pravděpodobně potrvá roky. Neexistuje rychlá a snadná implementace architektury Zero Trust."

Jeho kolega, finanční senior viceprezident, souhlasí. „Myslím, že to nikdy neskončí, protože se stále objevují nové technologie, nový malware a nové hrozby," říká.

Většina respondentů průzkumu (72 %) uvedla, že jejich harmonogramy zavádění probíhají podle plánu nebo s předstihem. Zbytek uvedl, že zavádění trvá déle, než se očekávalo.

Splňuje architektura Zero Trust vaše časové cíle?



Zdroj: Zero Trust Adoption Survey, březen 2022, Foundry. Základ: 168

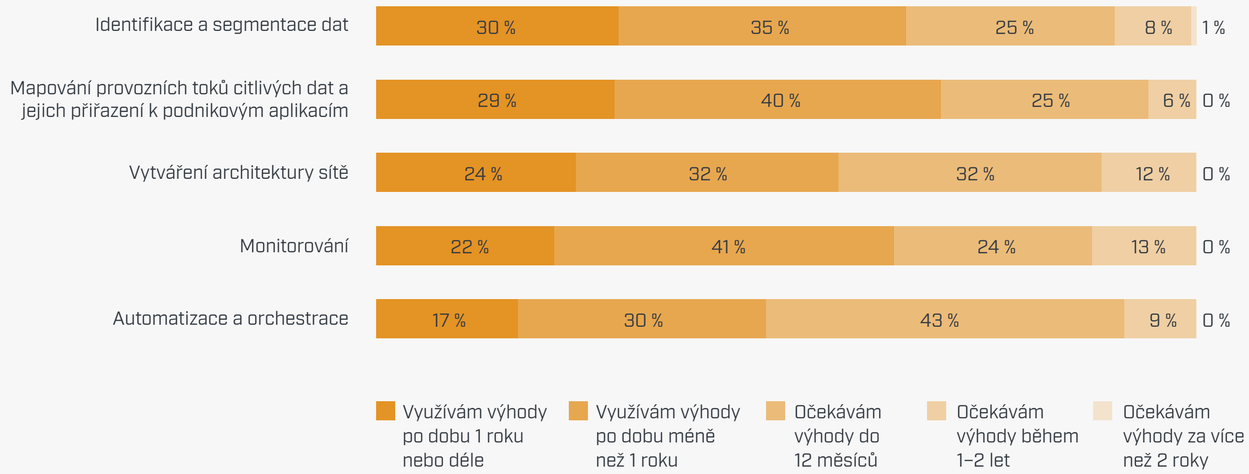
CSO Microsoft Security

Měřte za pochodu

Zatímco probíhá zavádění architektury Zero Trust, CISO mohou a měli by vytvořit milníky na této cestě, aby mohli měřit pokrok. Přibližně dvě třetiny respondentů průzkumu uvedly, že do jednoho roku získaly přínosy z většiny aspektů svých projektů. To je dobré znamení. Další čtvrtina nebo více respondentů očekává, že se jim to podaří do 12 měsíců, a to v rámci klíčových činností, jako je identifikace a segmentace dat, mapování přepravních toků a architektura sítě.

„Zero Trust je cesta, protože je třeba neustále vyhodnocovat, jak se bránit proti měnící se povaze útoků," říká Mocny. „Vždy se snažte o zlepšení."

Časový plán pro využití výhod architektury Zero Trust



Zdroj: Zero Trust Adoption Survey, březen 2022, Foundry. Základ: 103

Zaměřte se na lidi, nejen na technologie

Široký dosah modelu zabezpečení Zero Trust má dopad na každého zaměstnance, včetně týmů IT a bezpečnostních týmů pověřených jeho nasazením. Proto je stejně jako u každého velkého technologického projektu důležité zajistit, aby bylo nasazení synchronizováno s novými procesy i postupy řízení změn, a zajistit tak hladké a úspěšné zavedení.

„Kromě technologické změny dochází také ke změně kulturní," říká Mocny. Pokud máte více týmů zabývajících se zabezpečením (včetně síťových architektů nebo odborníků na identitu) musíte také změnit způsob, jakým tyto týmy spolupracují. Je třeba odstranit jednotlivá sila a zajistit, aby všechny technologie fungovaly dohromady."

Eliminace sil zahrnuje úzké zapojení týmů ze všech těchto oborů do pilotních projektů a testování konceptu (POC). Ředitel systémů IT v telekomunikační společnosti s přibližně 2 000 zaměstnanci se to naučil poté, co se během nasazení potýkal s několika samostatnými body selhání, včetně služeb, které nebylo možné ověřit a staly se náhle „nedůvěryhodnými". To způsobilo jejich nedostupnost, stejně jako nedostupnost některých systémů.

„Nasazení jedné služby může mít dominový efekt a způsobit pád ostatních," říká. Do budoucna „budeme mnohem opatrnější – více času na POC, více kontrol a více kontrol architektury s odborníky na danou oblast před nasazením."

Návratnost investice do architektury Zero Trust

Studie Forrester Consulting Total Economic Impact™ z roku 2021 vyčísluje úspory nákladů a obchodní přínosy řešení Microsoft Zero Trust. Na základě pěti podniků, s nimiž společnost Forrester vedla rozhovory, dosáhla složená organizace tříleté návratnosti investic ve výši 92 % díky implementaci architektury Zero Trust ve spolupráci s Microsoftem.

Tato složená organizace také ušetřila v průměru 20 USD na zaměstnance měsíčně tím, že se zbavila potřeby nástrojů zabezpečení, které se v rámci architektury Zero Trust staly nadbytečnými, včetně správy koncových bodů, antivirových a antimalwarových řešení.

CSO Microsoft Security

V jaké fáze nasazení modelu Zero Trust se nacházíte?

Jak vyplývá z průzkumu, výhody modelu zabezpečení Zero Trust jednoznačně převažují nad některými problémy, kterým CISO a jejich bezpečnostní týmy čelí při nasazování. Řešení těchto problémů pomocí dobře promyšleného plánu může vaší organizaci pomoct rychle zlepšit ochranu, snížit rizika a začít přinášet hodnotu v rámci celého podniku.

Pokud chcete vyhodnotit úroveň vyspělosti své organizace v oblasti architektury Zero Trust a získat další praktické zdroje pro nasazení, vyzkoušejte **hodnocení vyspělosti modelu Zero Trust** od Microsoftu.