Microsoft

Plán modelu nulové důvěry (Zero Trust)

Praktický průvodce implementací modelu nulové důvěry ve vaší organizaci

Obsah

Digitální transformace utváří nový normál

Organizace podstupují digitální transformaci, aby zvládly neustálé změny firemního prostředí:

- → Změny obchodních modelů a partnerství
- → Technologické trendy
- → Regulační, geopolitické a kulturní vlivy

Práce na dálku během pandemie COVID-19 urychlila transformaci a také způsobila, že se ze zabezpečení stala namísto pouhého nákladového střediska strategická hnací síla růstu.

COVID všem ukázal, že mohou nastat nepředvídané problémy a že se v budoucnu budete muset umět velmi rychle přizpůsobit. Čím více se budeme blížit modelu nulové důvěry, tím méně bude záležet na tom, jestli budeme fungovat z garáže, cloudu nebo datového centra.“

– Manažer, řešení identit a přístupu ve společnosti poskytující finanční služby

”

Například společnost H&R Block využila nástroje od Microsoftu k zavedení principů nulové důvěry během pouhých dvou týdnů, což umožnilo tisícům daňových specialistů bezpečně pracovat z domova.“

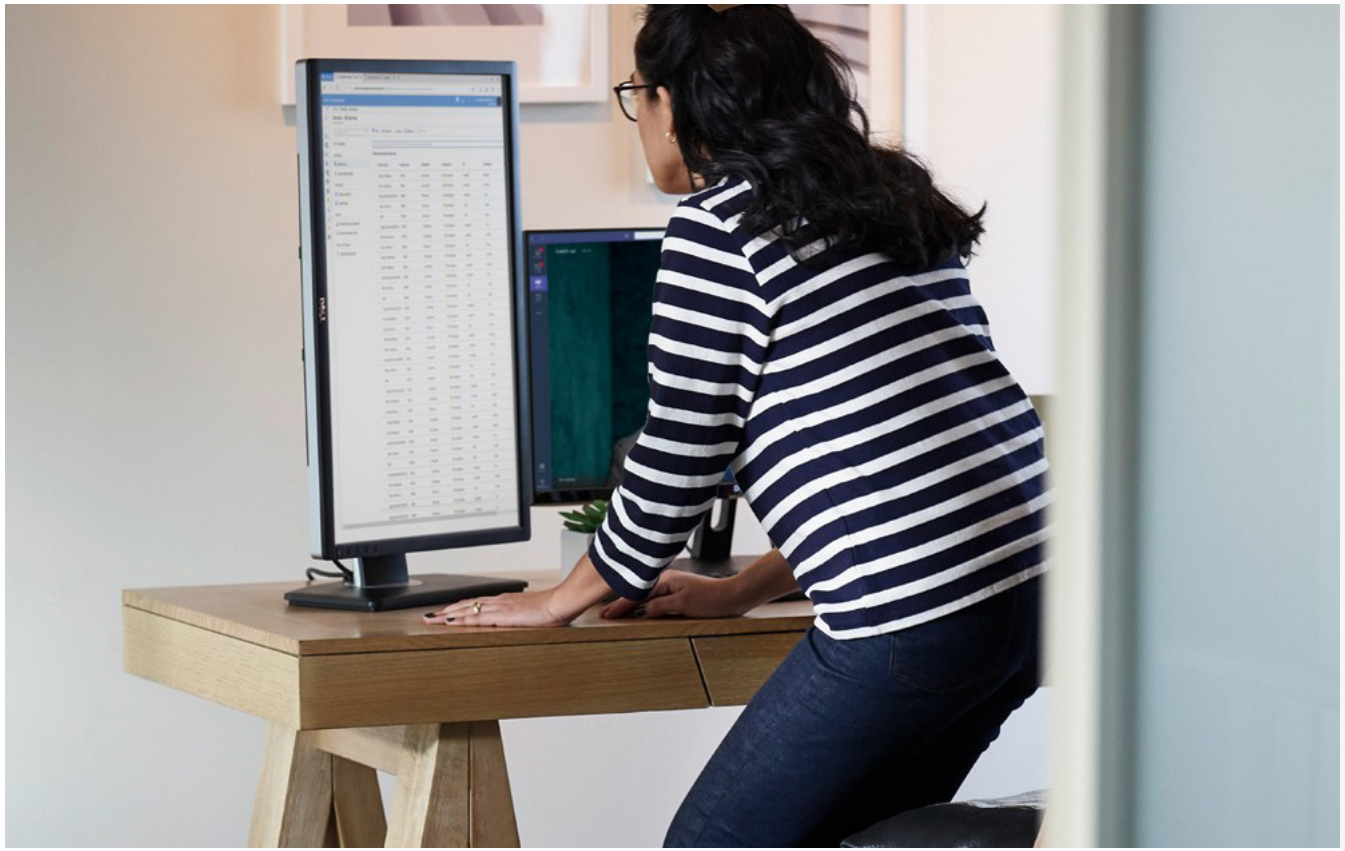
Zabezpečení digitální transformace vyžaduje nulovou důvěru

Digitální transformace si vynucuje přehodnocení tradičních modelů zabezpečení

Starší způsob zabezpečení nezajišťuje firmě flexibilitu, požadovaná uživatelská prostředí ani ochranu potřebnou pro rychle se rozvíjející digitální prostředky. Mnoho organizací implementuje model nulové důvěry, který jim pomáhá tyto problémy řešit a umožňuje jim přizpůsobit se novému standardu práce odkudkoli, s kýmkoli a kdykoli.

Tyto poznatky a osvědčené postupy vycházejí z rozhovorů se zákazníky a z našich vlastních zkušeností s implementací modelu nulové důvěry ve společnosti Microsoft.

Pragmatické přijetí modelu nulové důvěry: Myslete ve velkém, začněte v malém, postupujte rychle



Vypracujte víceletý plán pro tyto oblasti:

Stanovení priority rychlých úspěchů
a postupného pokroku pro každou iniciativu

Využívání stávajících technologií,
které už jsou nasazené nebo licencované

Strukturování ucelených iniciativ
s jasnými výsledky, výhodami a vlastnictvím

Přijetí modelu nulové důvěry

Vytvořili jsme použitelný rámec osvědčených postupů, který vám pomůže na vaší cestě k modelu nulové důvěry. Každá fáze obsahuje pokyny, osvědčené postupy, zdroje informací a nástroje, které vám pomohou řídit vlastní implementaci.

01 Plánování

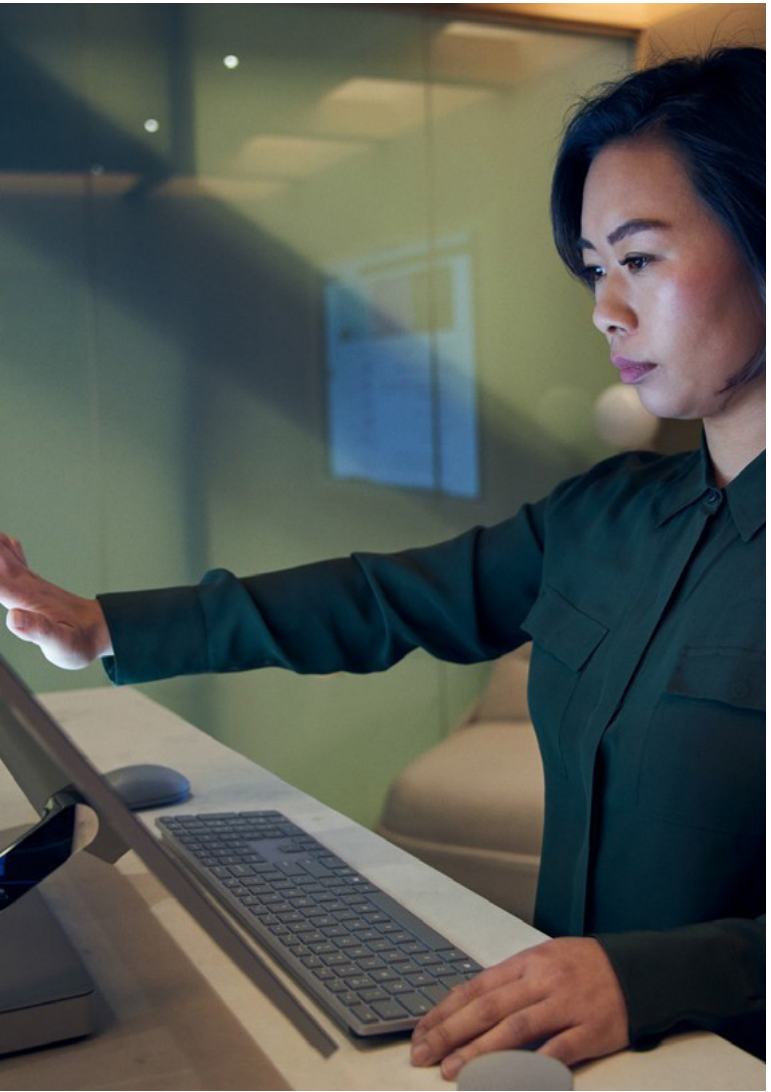
Vypracujte projektový záměr (business case) zaměřený na výsledky, které nejlépe odrážejí rizika a strategické cíle vaší organizace.

02 Implementace

Vytvořte víceletou strategii pro nasazení modelu nulové důvěry a stanovte priority včasných opatření na základě potřeb firmy.

03 Měření

Sledujte úspěšnost nasazení modelu nulové důvěry, abyste měli jistotu, že jeho implementace přináší měřitelná zlepšení.



Plán modelu nulové důvěry: Jak to má správně vypadat

Doporučené stanovení priorit:

→ **Definujte vizi** – nulová důvěra je mnohostranná cesta, která může trvat mnoho let. Jasné **definování** cílů, výsledků a architektury zajišťuje organizacím větší úspěch než reaktivní přístup.

Poznámka: Přínosy a implementace se často velmi liší v závislosti na vašich rolích a pracovních povinnostech.

→ **Získejte podporu vedení firmy** – úspěšné implementace modelu nulové důvěry se zaměřují na obchodní výsledky, aby získaly podporu vedení firmy pro ambiciózní cíle, přidělování prostředků z rozpočtu a slaďování interních procesů.

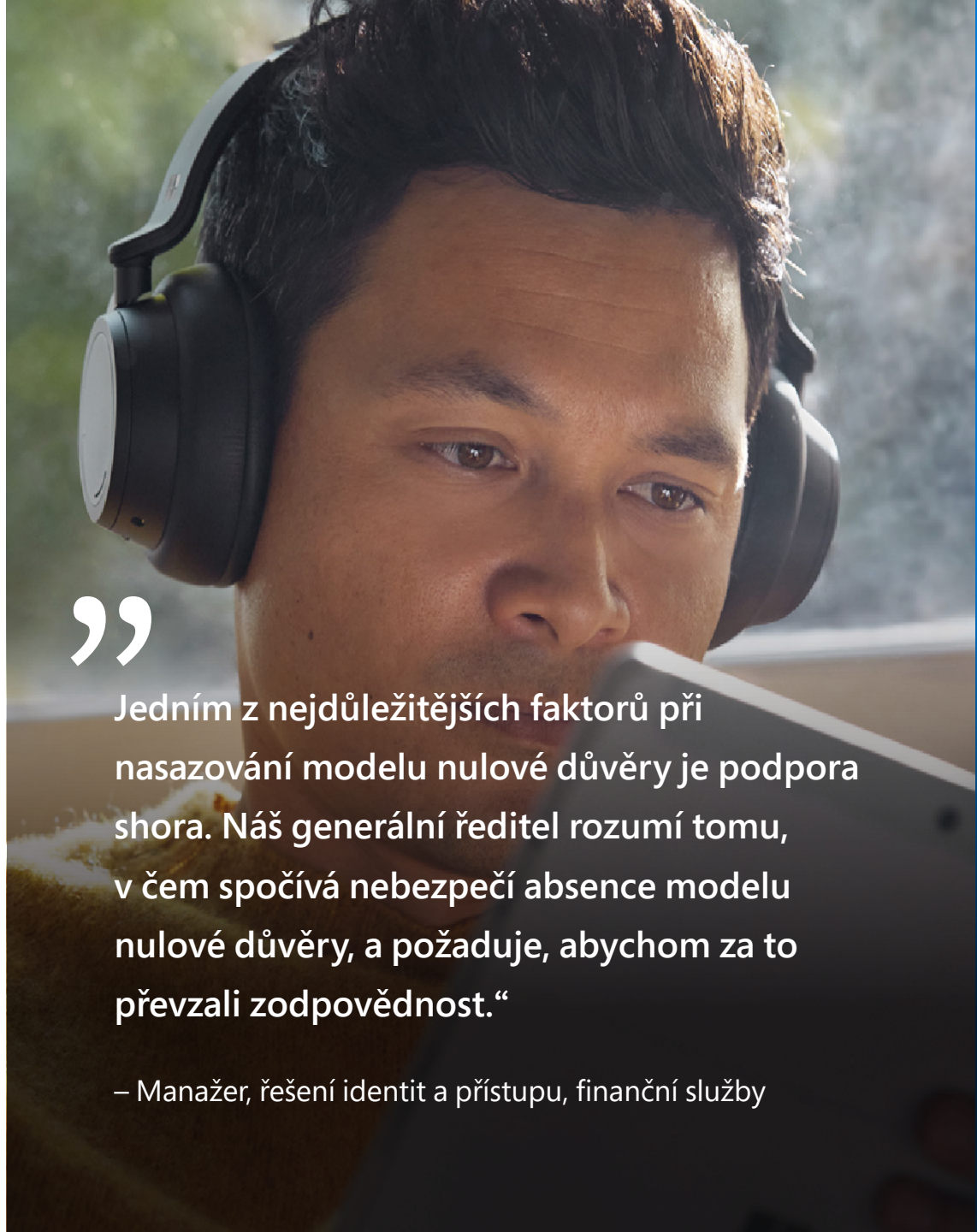
→ **Dejte koncovým uživatelům nové možnosti** – model nulové důvěry umožňuje technologickým týmům přímo spolupracovat s koncovými uživateli, aby se zabezpečení stalo hnací silou pro zlepšení jejich prostředí a produktivity.

Definování vize a získání podpory vedení firmy

Prvním krokem k získání podpory vedení je požádat o informace o prioritách firmy a pozorně si je vyslechnout a potom vytvořit vizi zaměřenou na požadované výsledky.

Tuto vizi je vždy nutné přizpůsobit prioritám firmy a firemní kultuře, přesto se v různých organizacích objevuje několik společných témat:

- → **Flexibilita firmy** z hlediska rychlého vyhledávání a využívání nových příležitostí při řízení rizik, zavádění možností práce na dálku a migraci do cloudu
- → **Správa složitého prostředí** souvisejícího s neustálými změnami obchodních partnerství, konkurence a dynamického technického prostředí
- → **Měřitelnost** k zajištění odpovědnosti za obchodní výsledky a zvládání rizik



Jedním z nejdůležitějších faktorů při nasazování modelu nulové důvěry je podpora shora. Náš generální ředitel rozumí tomu, v čem spočívá nebezpečí absence modelu nulové důvěry, a požaduje, abychom za to převzali zodpovědnost.“

– Manažer, řešení identit a přístupu, finanční služby

PLÁNOVÁNÍ 〉 IMPLEMENTACE 〉 MĚŘENÍ

Vypracování přesvědčivého projektového záměru zavedení modelu nulové důvěry

Přesvědčivý projektový záměr vám pomůže získat podporu vedení firmy a dosáhnout souladu napříč různými funkcemi ve firmě. Model zabezpečení na bázi nulové důvěry má mnoho výhod, organizace ovšem obvykle dosahují největšího úspěchu s následujícími čtyřmi projektovými záměry:

- → Podpora práce odkudkoli a kdykoli
- → Možnosti bezpečné a rychlé migrace do cloudu
- → Úspora nákladů díky zjednodušení systému zabezpečení

Zaměřte se na výsledné výhody pro firmu, včetně následujících:

- → **Proaktivní předcházení rizikům** a řízení rizik
- → **Řízení rizik pro partnery** se slabými programy zabezpečení
- → **Flexibilita v oblasti zabezpečení a dodržování předpisů, která umožňuje přizpůsobit se rychlým změnám stavu rolí a organizací**

Implementace modelu nulové důvěry: Jak to má správně vypadat

Strukturujte program do jasných a ucelených iniciativ. Společnost Microsoft zjistila, že technické strategie a architektury se přirozeně seskupují do těchto iniciativ v oblasti zabezpečení:

- Zabezpečení produktivity
- Moderní provoz zabezpečení
- Operační technologie (OT) a Internet věcí (IoT), *pokud jsou pro danou organizaci relevantní*
- Datové centrum, služby a rozhraní API

Tyto údaje vychází ze zkušeností společnosti Microsoft a dalších úspěšných implementací u zákazníků.

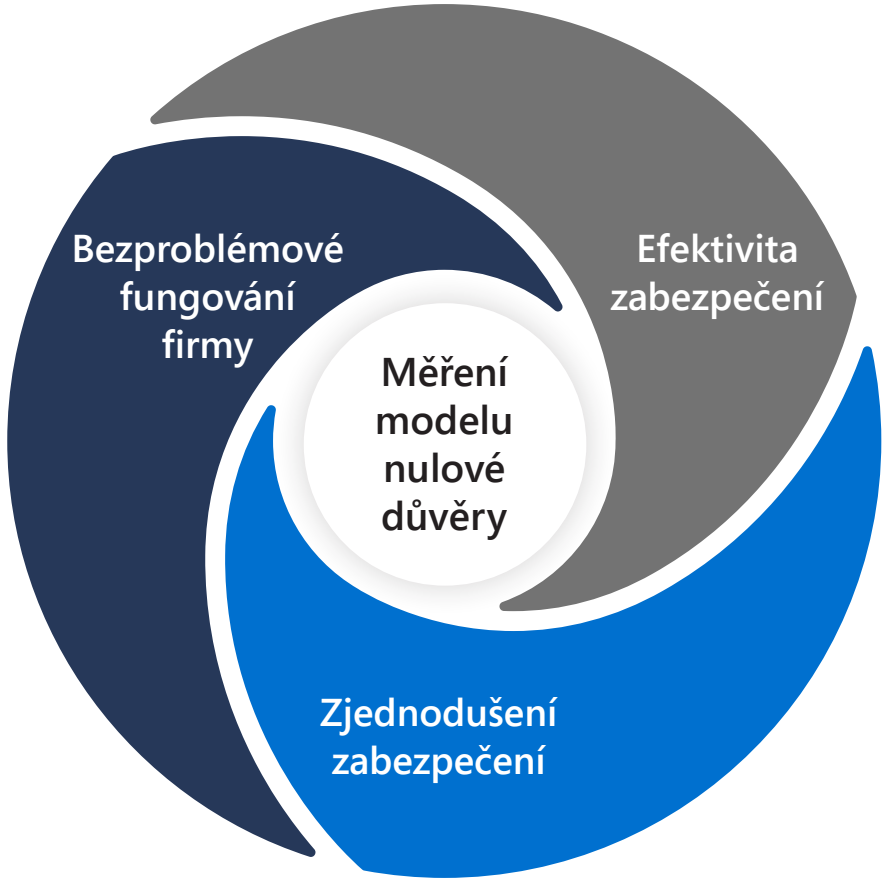
Stanovení priorit a plánování iniciativ:

- **Posuďte každou iniciativu z hlediska cílů firmy** a vyhodnoťte potenciální pozitivní dopady na firmu, třecí plochy a problémy.
- **Vytvořte krátkodobý plán.** Začněte aktivitami, které mohou přinést rychlé úspěchy, a najděte si osoby z vedení firmy, které vás budou podporovat.
- **Vypracujte dlouhodobý plán.**

Měření pokroku – jak to má správně vypadat

Identifikujte klíčové milníky a výkonnostní cíle pro svou organizaci, měřte je a informujte o úspěších a získaných poznatcích.

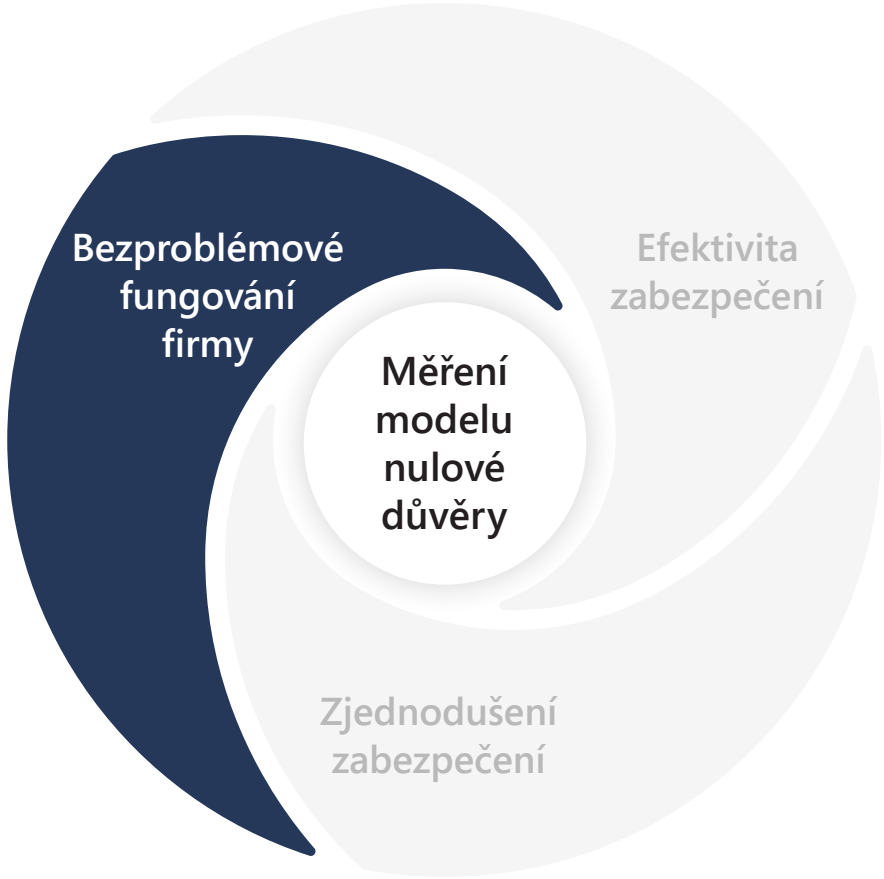
- **Bezproblémové fungování firmy** – měření třecích ploch v uživatelském prostředí a toho, jak dlouho trvá schvalování iniciativ v rámci interního zabezpečení
- **Efektivita zabezpečení** – identifikace snižování počtu incidentů zabezpečení nebo dopadů těchto incidentů poté, co organizace přijala strategii nulové důvěry
- **Zjednodušení zabezpečení** – omezení počtu dodavatelů zabezpečení, které musí týmy integrovat, a snižování nákladů na ručně prováděné úlohy (například volání kvůli resetování hesla)



Měření zlepšování fungování firmy

Model nulové důvěry by měl umožňovat bezproblémové fungování prostředí pro uživatele a vývojáře:

- Počet přerušení pracovního postupu uživatelů z důvodu zabezpečení (například, kolikrát za den se zobrazí výzva vícefaktorového ověřování)
- Milníky nasazení (například procento zaměstnanců, kteří získávají přístup k aplikacím prostřednictvím jednotného přihlašování)
- Milníky viditelnosti (například pokles v používání aplikace v důsledku špatného uživatelského prostředí pro přihlášení)
- Průměrná doba spouštění spravovaných zařízení v sekundách
- Průměrný počet dnů pro vyhodnocení aplikací z hlediska zabezpečení



Nezapomeňte na mechanismy naslouchání koncovým uživatelům a provádějte průzkumy mezi uživateli ohledně toho, jak snadné je používat přístup, proces resetování hesel a další funkce.

Měření efektivity zabezpečení

Měření stavu zabezpečení a výsledného dopadu incidentů zabezpečení:

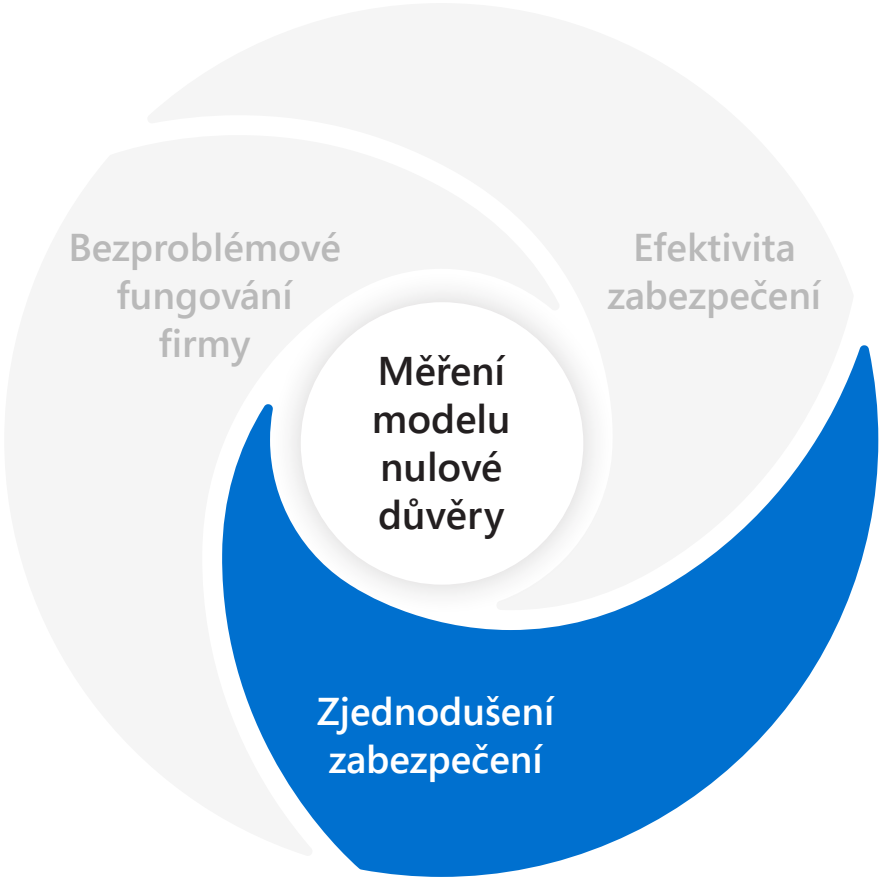
- Počet incidentů zabezpečení (podle závažnosti)
- Milníky nasazení (například procento zaměstnanců, kteří aktivně používají vícefaktorové ověřování)
- Milníky viditelnosti (například procento spravovaných zařízení nebo aplikací)
- Stav zabezpečení – sledování zlepšování v Microsoft Secure Score

Mějte přehled o kontextu: S modelem nulové důvěry získáte lepší přehled o celém prostředí, proto můžete zjišťovat více incidentů, které jste dříve neodhalili.

Měření zjednodušení zabezpečení

Model nulové důvěry často pomáhá zjednodušit požadavky na dosažení zabezpečení

- Počet duplicitních nástrojů zabezpečení, které provádí podobné nebo stejné funkce
- Počet nástrojů zabezpečení, které vyžadují vlastní integraci
- Procento času, které IT helpdesk věnoval aktivitám s nízkou hodnotou, jako je resetování hesla
- Počet ručních kroků u opakujících se pracovních postupů (například prověřování běžných upozornění nebo incidentů, ruční zřizování uživatelů, úlohy generování sestav o dodržování předpisů)
- Procento falešně pozitivních upozornění prověřovaných týmy zabezpečení
- Poměr času stráveného údržbou nástrojů a skutečnými reakcemi na incidenty



Nulová důvěra je klíčovou funkcí zajišťující úspěch digitální transformace

Pokud chcete začít, nemusíte nahrazovat stávající technologie.

Začněte tím, že přizpůsobíte svoje investice do modelu nulové důvěry aktuálním potřebám firmy a zaměříte se na dosažení rychlých výsledků. Každý úspěch postupně přináší přidanou hodnotu pro snížení rizika a zlepšení stavu zabezpečení vašich digitálních prostředků.

Nikdy není pozdě začít a žádný rozsah není příliš malý.

> Od doby, kdy jsme implementovali strategii nulové důvěry s technologiemi Microsoftu 365, si mohou naši zaměstnanci plnit firemní povinnosti odkudkoli na světě a my si přitom udržujeme pevnou kontrolu nad klíčovými požadavky na zabezpečení.“

– Igor Tsyganskiy, ředitel pro technologie, Bridgewater Associates

Kam dál?

Děkujeme, že jste si prošli našeho průvodce osvědčenými postupy pro model nulové důvěry. Pokud jste to ještě neudělali, přečtěte si náš dokument o modelu vyspělosti nulové důvěry (kliknutím stáhnete), který podrobně popisuje základní principy nulové důvěry a náš model vyspělosti rozdělující požadavky na nejvyšší úrovni do šesti základních prvků.

Na našem externím webu Microsoft Zero Trust jsme také shromáždili užitečné poznatky, odbornou dokumentaci a další materiály.


Microsoft