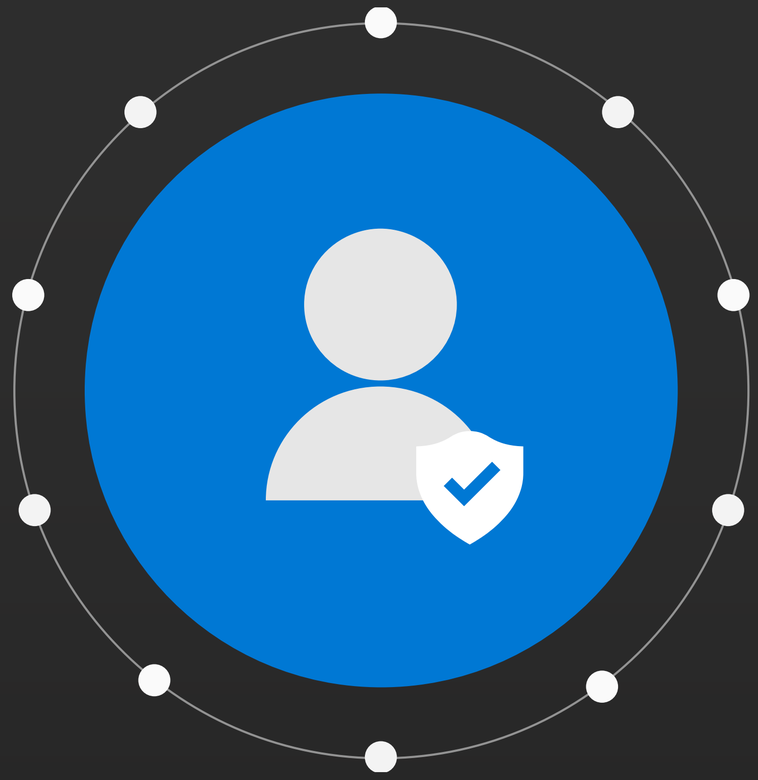
Microsoft 365

10 tipů pro zabezpečení typu nulová důvěra (zero trust)



10 tipů pro zabezpečení typu nulová důvěra (zero trust)

Veřejné cloudové služby jsou stále rozšířenější, roste počet mobilních pracovníků a v důsledku toho modely zabezpečení založené na ochraně perimetru už nevyhovují novým podmínkám. Aplikace a data organizací se dnes vyskytují uvnitř i vně tradiční brány firewall. Bezpečnostní týmy a IT oddělení už dnes nemohou předpokládat, že uživatelé a jejich zařízení (osobní i firemní) ve firemní síti jsou bezpečnější než ti, kteří se nacházejí mimo ni. Ovládací prvky perimetru nemohou zabránit útočníkovi v taktice lateral movement v síti poté, co do ní získá přístup.

Je tedy třeba přejít na zabezpečení „bez hranic“, které je známější pod názvem zero trust – model nulové důvěry. V modelu nulové důvěry se všichni uživatelé a všechna zařízení – uvnitř i vně firemní sítě – považují za nedůvěryhodné. Přístup se uděluje na základě dynamického vyhodnocování rizik spojených s každou žádostí. Pro všechny uživatele, zařízení, aplikace a data se vždy používají stejné kontroly zabezpečení.

Model nulové důvěry (zero trust) je stále oblíbenější

Zájem o model nulové důvěry roste. Nový průzkum společnosti IDG ukázal, že 21 % organizací už model nulové důvěry přijalo a 63 % to v následujících 12 měsících plánuje udělat[1]. V jiném průzkumu společnosti IDG z roku 2018, který se týkal priorit v oblasti zabezpečení, 35 % organizací uvedlo, že plánují zvýšit výdaje na model nulové důvěry nebo pro něj vytvořit novou kategorii výdajů. Dalších 30 % považuje model nulové důvěry za potenciální novou oblast pro investice[2].

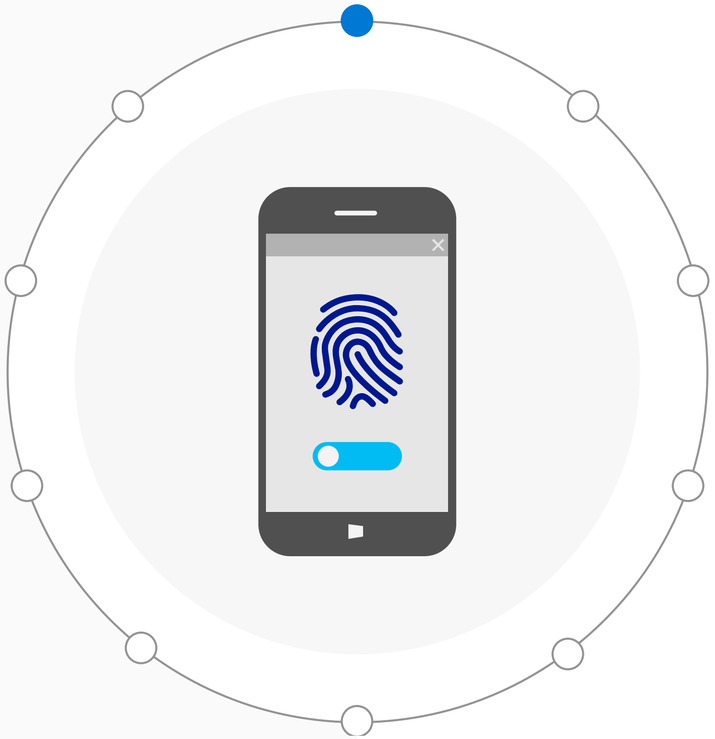
Model nulové důvěry si dnes získává širokou oblibu, není to ovšem nový přístup. V roce 2004 bylo založeno bezpečnostní konsorcium s názvem Jericho Forum, které propagovalo myšlenku tzv. deperimetrizace (odstranění hranic mezi organizací a vnějším světem) související s hledáním nových způsobů ochrany dat na nových platformách[3]. Analytická firma Forrester poprvé použila termín zero trust v roce 2010[4].

Zájem o model nulové důvěry v poslední době roste, a to zejména mezi organizacemi, které potřebují zajistit ochranu před útočníky využívajícími v síti taktiku lateral movement.

Přechod na model nulové důvěry může vyžadovat roky úsilí a také spolupráci napříč celou organizací. Pokud jste se rozhodli nasadit model nulové důvěry nebo o tom uvažujete, podívejte se na 10 tipů, které vám tuto cestu usnadní.

Tip č. 1

Zaměřte se na identity



Nejlepším výchozím bodem pro model nulové důvěry je využití identit.

Uživatelé mohou mít několik zařízení a přístup k firemním prostředkům z různých sítí a aplikací.

Tip č. 1

Zaměřte se na identity

Nejlepším výchozím bodem pro model nulové důvěry je využití identit.

Uživatelé mohou mít několik zařízení a přístup k firemním prostředkům z různých sítí a aplikací. Téměř všechny tyto prostředky vyžadují ověřování, proto je identita společným jmenovatelem všech žádostí o přístup – ať už z osobního zařízení ve veřejné síti Wi-Fi, nebo z firemního zařízení, které se nachází uvnitř perimetru sítě. Použití identity jako řídicí roviny umožňuje organizacím považovat každou žádost o přístup za nedůvěryhodnou, dokud nedojde k plnému ověření uživatele, zařízení nebo jiných faktorů.

Mnoho organizací se zaměřuje na zavedení modelu nulové důvěry prostřednictvím mikrosegmentace, ale tento přístup má významná omezení.

Mikrosegmentace může být užitečná ke snižování počtu potenciálních oblastí útoku a k tomu, abyste zabránili porušení zabezpečení v místních prostředích se staršími aplikacemi.

Tento přístup ovšem není tak efektivní v cloudových prostředích, kde příslušná IT oddělení často nevlastní ani nespravují sítě mezi firemními prostředky.

Model nulové důvěry představuje posun od síťových ovládacích prvků k zásadám a procesům založeným na identitách. Týmy s různými specializacemi by měly spolupracovat na vytváření ochrany založené na identitách a vytvořit tak základ pro model nulové důvěry. „Vybudování základu založeného na identitách je nejlepším výchozím bodem," říká Mark Simos, hlavní architekt skupiny vyvíjející řešení pro kybernetickou bezpečnost v Microsoftu. „Identita vytvoří dobrou přístupovou bránu, která chrání vaše prostředky před potenciálními hrozbami."

Tip č. 2

Implementujte řízení podmíněného přístupu

Hackeři běžně zneužívají přihlašovací údaje identit a používají je k přístupu k systémům a k taktice lateral movement v síti.

Důvěryhodnost určitého zařízení nebo uživatele nelze tedy odvozovat jenom z toho, jestli se nachází uvnitř podnikové sítě nebo mimo ni.

Tip č. 2

Implementujte řízení podmíněného přístupu

Hackeři běžně zneužívají přihlašovací údaje identit a používají je k přístupu k systémům a k taktice lateral movement v síti.

Důvěryhodnost určitého zařízení nebo uživatele nelze tedy odvozovat jenom z toho, jestli se nachází uvnitř podnikové sítě nebo mimo ni.

Namísto toho je třeba **uplatňovat přístup, který vždy předpokládá porušení zabezpečení, a nedůvěřovat žádné žádosti, dokud není plně prověřená.** U modelu nulové důvěry by rozhodování týkající se řízení přístupu mělo být dynamické a přístup by měl být udělován podmíněně na základě vyhodnocení a pochopení kontextu rizika spojeného s každou žádostí prostředku v různých dimenzích.

Tato metoda podmíněného přístupu zohledňuje identitu a přístupová práva uživatele, stav zařízení, bezpečnost aplikací a sítí a citlivost dat, ke kterým je přístup povolován.

K rozhodování o tom, jestli se povolí, zakáže nebo zablokuje přístup k požadovanému prostředku, se potom použije vynucovací modul ovládaný sadou podrobných zásad. Síť s nulovou důvěrou se správnými zásadami podmíněného přístupu pro uživatele a zařízení může zabránit hackerům v používání odcizených přihlašovacích údajů k taktice lateral movement v síti.

Tip č. 3

Používejte silné přihlašovací údaje

Slabá hesla ohrožují zabezpečení systému identit a usnadňují hackerům zneužití sítě, například prostřednictvím útoků password spray nebo credential stuffing.

Tip č. 3

Používejte silné přihlašovací údaje

Slabá hesla ohrožují zabezpečení systému identit a usnadňují hackerům zneužití sítě, například prostřednictvím útoků password spray nebo credential stuffing.

Pokud použijete vícefaktorové ověřování jako součást omezení v rámci podmíněného přístupu, docílíte lepšího ověřování uživatelů a zabráníte hackerům ve zneužití odcizených přihlašovacích údajů.

Vícefaktorové ověřování vám umožní použít další vrstvu ověřování uživatelů – zejména pro přístup k důležitým aplikacím a datům.

Tip č. 4

Naplánujte strategii dvojího perimetru

Pokud chcete předejít výpadkům ve fungování služeb a vyhnout se starým rizikům, zachovejte stávající síťovou ochranu a přidejte do svého prostředí nové ovládací prvky založené na identitách.

Tip č. 4

Naplánujte strategii dvojího perimetru

Pokud chcete předejít výpadkům ve fungování služeb a vyhnout se starým rizikům, zachovejte stávající síťovou ochranu a přidejte do svého prostředí nové ovládací prvky založené na identitách.

„V kontextu modelu nulové důvěry opravdu musíte začít posuzovat svoje aplikace podle toho, jestli jsou cloudové, nebo starší," říká Simos. Cloudové aplikace podporují ovládací prvky založené na identitách a umožňují poměrně snadno vrstvit zásady podmíněného přístupu.

Další kategorii tvoří aplikace navržené tak, aby fungovaly za síťovými bránami firewall ve starších prostředích.

Tyto aplikace je třeba modernizovat, aby podporovaly podmíněný přístup založený na identitách. Jednou z možností, jak toho v požadovaném měřítku dosáhnout, je povolit přístup prostřednictvím zabezpečené brány pro ověřování nebo proxy aplikací. Díky tomu také můžete eliminovat sítě VPN (to vám může pomoct snížit riziko).

Tip č. 5

Integrujte analýzu hrozeb a chování

Podpora řízení přístupu založeného na identitách, kterou nabízejí cloudové aplikace, není jediným důvodem, proč byste měli urychlit migraci do cloudu.

Cloud také generuje bohatší telemetrii, která umožňuje lepší rozhodování v rámci řízení přístupu. Tato telemetrie může například zdokonalit řízení podmíněného přístupu tím, že usnadňuje zjišťování neobvyklého chování uživatele nebo entity a umožňuje tak identifikovat hrozby.

Tip č. 5

Integrujte analýzu hrozeb a chování

Podpora řízení přístupu založeného na identitách, kterou nabízejí cloudové aplikace, není jediným důvodem, proč byste měli urychlit migraci do cloudu.

Cloud také generuje bohatší telemetrii, která umožňuje lepší rozhodování v rámci řízení přístupu. Tato telemetrie může například zdokonalit řízení podmíněného přístupu tím, že usnadňuje zjišťování neobvyklého chování uživatele nebo entity a umožňuje tak identifikovat hrozby.

Vaše možnosti rozhodování v rámci řízení přístupu závisejí na kvalitě, kvantitě a rozmanitosti signálů, které do tohoto rozhodování integrujete.

Integrace zdrojů pro analýzu hrozeb, například IP adres pro roboty nebo malware, donutí útočníky neustále získávat nové prostředky. Pokud integrujete další podrobnosti o přihlášení (čas, místo atd.) a budete zjišťovat, jestli odpovídají obvyklému chování uživatele, bude to pro útočníky obtížnější napodobit a zároveň tak minimalizujete nepohodlí pro uživatele.

Tip č. 6

Omezte potenciální oblast útoku

Pokud chcete zlepšit zabezpečení infrastruktury identit, je důležité minimalizovat potenciální oblast útoku. (I obecně je to dobré bezpečnostní opatření.)

Například implementací privilegované správy identit minimalizujete pravděpodobnost použití napadeného účtu v roli správce nebo v jiné privilegované roli.

Tip č. 6

Omezte potenciální oblast útoku

Pokud chcete zlepšit zabezpečení infrastruktury identit, je důležité minimalizovat potenciální oblast útoku. (I obecně je to dobré bezpečnostní opatření.)

Například implementací privilegované správy identit minimalizujete pravděpodobnost použití napadeného účtu v roli správce nebo v jiné privilegované roli.

Doporučujeme také blokovat aplikace používající starší ověřovací protokoly.

Je to důležité, protože tyto protokoly nepodporují podmíněný přístup ani vícefaktorové ověřování, což útočníkům umožňuje, aby je obešli.

Omezte také přístupové body pro ověřování, abyste měli kontrolu nad tím, jak uživatelé přistupují k aplikacím a prostředkům. To také pomůže snížit dopad zneužití napadených přihlašovacích údajů.

Tip č. 7

Zvyšujte povědomí o zabezpečení

Infrastruktura identit a koncových bodů může generovat velké množství událostí a výstrah zabezpečení.

K agregaci a korelaci dat používejte systém pro správu akcí a informací o zabezpečení (SIEM). To vám pomůže snadněji rozpoznávat podezřelé aktivity a vzorce, které naznačují možné vniknutí do sítě a události jako únik přihlašovacích údajů, chybné IP adresy a přístup z infikovaných zařízení.

Tip č. 7

Zvyšujte povědomí o zabezpečení

Infrastruktura identit a koncových bodů může generovat velké množství událostí a výstrah zabezpečení.

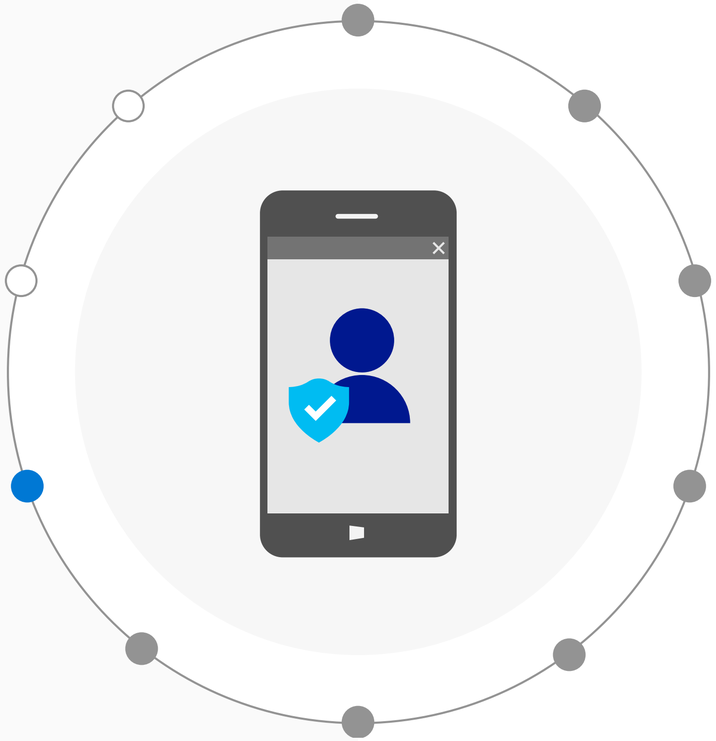
K agregaci a korelaci dat používejte systém pro správu akcí a informací o zabezpečení (SIEM). To vám pomůže snadněji rozpoznávat podezřelé aktivity a vzorce, které naznačují možné vniknutí do sítě a události jako únik přihlašovacích údajů, chybné IP adresy a přístup z infikovaných zařízení.

Pomocí systému SIEM můžete auditovat aktivity uživatelů, dokumentovat dodržování předpisů a usnadňovat forenzní analýzu.

Tento systém také může zlepšit monitorování nejméně privilegovaného přístupu a zajistit, aby uživatelé měli přístup jenom k prostředkům, které opravdu potřebují.

Tip č. 8

Povolte samoobslužné funkce pro koncové uživatele



Zavedení modelu nulové důvěry se pravděpodobně nesetká u uživatelů s takovým odporem, jaký vyvolávají jiné iniciativy v oblasti zabezpečení.

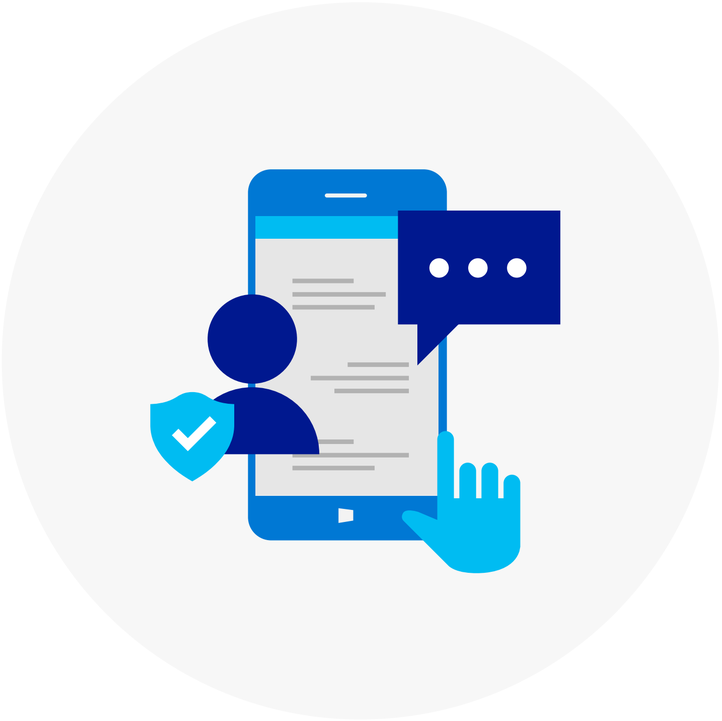
Uživatelé už totiž přístup založený na identitách znají ze svých osobních zařízení a aplikací a chtějí používat stejné prostředí i v práci. Model nulové důvěry umožňuje organizacím zajišťovat zabezpečení moderních scénářů pro zvyšování produktivity, jako například používání mobilních zařízení, práce zaměstnanců na vlastních zařízeních (BYOD) a aplikace SaaS. Zajistíte tak, aby uživatelé byli spokojenější, ale zároveň neohrozíte zabezpečení.

Tip č. 8

Povolte samoobslužné funkce pro koncové uživatele

Zavedení modelu nulové důvěry se pravděpodobně nesetká u uživatelů s takovým odporem, jaký vyvolávají jiné iniciativy v oblasti zabezpečení.

Uživatelé už totiž přístup založený na identitách znají ze svých osobních zařízení a aplikací a chtějí používat stejné prostředí i v práci. Model nulové důvěry umožňuje organizacím zajišťovat zabezpečení moderních scénářů pro zvyšování produktivity, jako například používání mobilních zařízení, práce zaměstnanců na vlastních zařízeních (BYOD) a aplikace SaaS. Zajistíte tak, aby uživatelé byli spokojenější, ale zároveň neohrozíte zabezpečení.



IT týmy mohou zajistit hladší fungování procesů tím, že umožní uživatelům provádět některé úlohy zabezpečení, například samoobslužné resetování hesel.

Pokud uživatelům umožníte, aby si sami resetovali nebo odemykali hesla ke svým účtům bez účasti správce, a zároveň budete tyto funkce monitorovat, aby nedošlo k jejich zneužití, dosáhnete rovnováhy mezi zabezpečením a produktivitou.

Pokud také implementujete samoobslužnou správu skupin, mohou vlastníci vytvářet a spravovat skupiny sami a nemusí to za ně dělat správce.

Tip č. 9

Neslibujte nereálné

Model nulové důvěry nespočívá v provedení jedné převratné změny, jako je například implementace vícefaktorového ověřování.

Jde spíše o dlouhodobou strategii, jejímž cílem je využívání ovládacích prvků zabezpečení nové generace, které fungují úplně jinak než tradiční síťové modely přístupu.

Tip č. 9

Neslibujte nereálné

Model nulové důvěry nespočívá v provedení jedné převratné změny, jako je například implementace vícefaktorového ověřování.

Jde spíše o dlouhodobou strategii, jejímž cílem je využívání ovládacích prvků zabezpečení nové generace, které fungují úplně jinak než tradiční síťové modely přístupu.

K tomu, abyste dosáhli určité vize, potřebujete čas. Je také vhodné postupovat prostřednictvím navazujících menších projektů.

V průběhu realizace je důležité vhodně stanovit a řídit cíle a očekávání. Je třeba získat podporu klíčových účastníků celého procesu a mít plán, jak s nimi efektivně komunikovat během celého životního cyklu projektu. Připravte si postup, jak překonávat různé překážky a odpor skupin uživatelů, kteří byli zvyklí dělat věci jinak.

Tip č. 10

Průběžně ukazujte přidanou hodnotu

Jedním z nejúčinnějších způsobů, jak získat dlouhodobou podporu pro zavedení modelu nulové důvěry, je ukázat přidanou hodnotu každého provedeného kroku.

V průzkumu společnosti IDG, který se týkal zabezpečení, více než polovina respondentů (51 %) uvedla, že model nulové důvěry by mohl zlepšit jejich možnosti chránit zákaznická data, a 46 % uvedlo, že by mohl zajistit lepší a bezpečnější prostředí pro koncové uživatele.

Tip č. 10

Průběžně ukazujte přidanou hodnotu

Jedním z nejúčinnějších způsobů, jak získat dlouhodobou podporu pro zavedení modelu nulové důvěry, je ukázat přidanou hodnotu každého provedeného kroku.

V průzkumu společnosti IDG, který se týkal zabezpečení, více než polovina respondentů (51 %) uvedla, že model nulové důvěry by mohl zlepšit jejich možnosti chránit zákaznická data, a 46 % uvedlo, že by mohl zajistit lepší a bezpečnější prostředí pro koncové uživatele.

Vaše možnosti rozhodování v rámci řízení přístupu závisejí na kvalitě, kvantitě a rozmanitosti signálů, které do tohoto rozhodování integrujete.

Integrace zdrojů pro analýzu hrozeb, například IP adres pro roboty nebo malware, donutí útočníky neustále získávat nové prostředky. Pokud integrujete další podrobnosti o přihlášení (čas, místo atd.) a budete zjišťovat, jestli odpovídají obvyklému chování uživatele, bude to pro útočníky obtížnější napodobit a zároveň tak minimalizujete nepohodlí pro uživatele.

Microsoft 365

Model pro budoucnost

Není možné předvídat, jaké nové typy zneužití se mohou každý den objevit a jak mohou získat přístup do vašeho prostředí. Nikdy si nemůžete být úplně jistí, jestli konkrétní uživatel, zařízení, aplikace nebo síť nepředstavuje riziko, proto lze za jediný uvážlivý přístup k zabezpečení považovat to, že nikomu nedůvěřujete a vše ověřujete.

Model nulové důvěry není snadné vybudovat, jde ale o klíčový prvek na jakékoli dlouhodobé cestě k modernizaci digitální organizace.

Další informace o řešení výzev v oblasti kybernetické bezpečnosti získáte tady:

Podívejte se na náš seriál Microsoft CISO Spotlight

[1] IDG Explorer survey, květen 2019
[2] IDG Security Priorities study, 2018, https://www.idg.com/tools-for-marketers/2018-security-priorities-study/
[3] Wikipedie, https://en.wikipedia.org/wiki/Jericho_Forum
[4] CSO, červenec 2018, https://www.csoonline.com/article/3287057/what-it-takes-to-build-a-zero-trust-network.html