Microsoft 365

Využití potenciálu AI s bezpečnými základy

Obsah

ÚVOD

Příležitost AI a nutnost zabezpečení

Mezi dnešními pracovníky se prohlubuje kapacitní mezera v oblasti produktivity. V nedávné zprávě Index pracovních trendů **více než 80 %** dotazovaných pracovníků se znalostmi ve 31 zemích – včetně zaměstnanců i vedoucích pracovníků – uvedlo, že jim chybí čas nebo energie na práci[1]. Zároveň **více než 50 %** dotazovaných vedoucích pracovníků firem uvedlo, že ke splnění cílů je třeba zvýšit produktivitu[1]. To představuje příležitost posoudit způsoby práce a potenciální řešení, která by nám pomohla tuto propast překlenout. AI, včetně agentů, představuje jako řešení velký potenciál. **Více než 80 %** oslovených vedoucích pracovníků uvedlo, že jsou přesvědčeni, že jejich organizace začnou v příštích 12–18 měsících používat agenty AI k rozšíření kapacity pracovní síly[1].

Tento spěch směrem k AI přichází s nevýhodou: inovace by měly být vyváženy robustním zabezpečením a ochranou dat, aby se zmírnila potenciální rizika. V nedávné studii iSMG **více než 70 %** oslovených vedoucích pracovníků uvedlo, že zajištění ochrany soukromí a zabezpečení dat představuje hlavní problém při integraci generativní AI do stávající infrastruktury IT[2]. Vedoucí pracovníci čelí dvěma problémům: urychlení zavedení AI ke zvýšení produktivity a ochrana dat v této nové éře.

Tato elektronická kniha vám poskytne informace o příkladech scénářů AI, které by mohly představovat potenciální rizika, tipy, jak tato rizika zmírnit pomocí Microsoft 365 E3, a kontrolní seznam, který organizacím pomůže začít přípravu na přijetí AI ve velkém nebo v ní pokračovat. Připravte se na zavedení AI s jistotou: umožníte své organizaci inovovat s AI, aniž by byly ohroženy standardy zabezpečení nebo dodržování předpisů v organizaci.

Dobré úmysly s potenciálním rizikem: Příklady scénářů AI

Největší rizika spojená s používáním a zaváděním AI jsou často spojena se zaměstnanci s dobrými úmysly, kteří se snaží dělat svou práci a zajistit větší dopad. V honbě za vyšší produktivitou mohou členové týmu neúmyslně sdílet citlivé informace s nástroji AI nebo používat aplikace, které ještě nejsou schváleny oddělením IT. To může vytvářet rizika a vystavovat organizaci novým hrozbám.

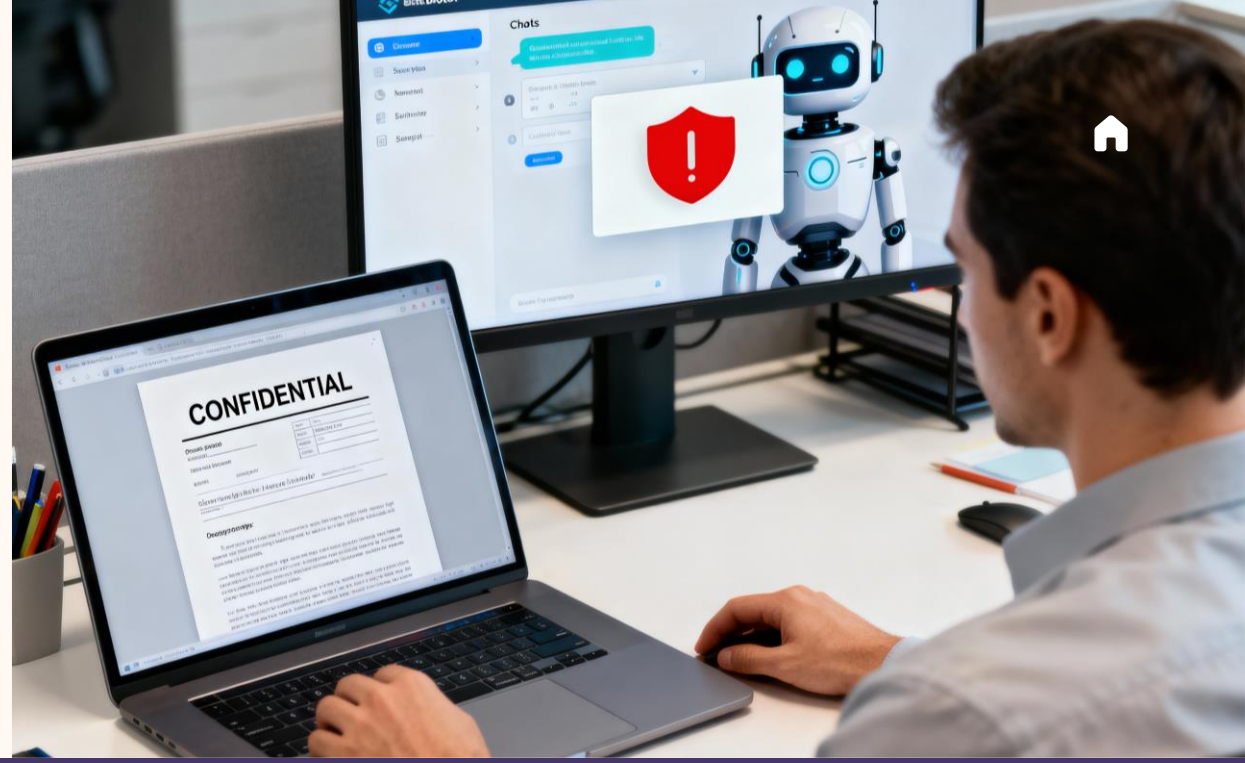
Podívejme se na dva ukázkové scénáře, které to ilustrují – jeden s kancelářským informačním pracovníkem a druhý s pracovníkem prvního kontaktu.

V těchto fiktivních příkladech se dozvíte: 1) jak dobře míněné použití AI může vést k ohrožení bezpečnosti, pokud není řádně spravováno, a 2) jak lze tato potenciální rizika zmírnit pomocí robustního základu zabezpečení.

1. ukázkový scénář[4]

Produktový marketingový manažer využívá nástroj s AI k přípravě tiskové zprávy

Produktový marketingový manažer ve výrobní společnosti je pod časovým tlakem, aby vypracoval tiskovou zprávu o uvedení nového produktu na trh v nadcházejících měsících. Aby získal nápady a urychlil proces psaní, tento zaměstnanec zkopíroval a vložil výňatky z důvěrné roadmapy produktu a interní finanční projekce do bezplatného online AI asistenta pro psaní. Nástroj s AI rychle vygeneruje několik propracovaných odstavců, které pak zaměstnanec použije v návrhu tiskové zprávy. Tento nástroj však dosud nebyl prověřen ani schválen jeho organizací.



Potenciální riziko:

Použitím této externí služby AI nahrál zaměstnanec citlivá firemní data (plány produktů a finanční informace) do systému třetí strany, nad kterým IT tým nemá kontrolu ani možnost správy. Jakmile jsou data sdílena s nástrojem s AI, společnost nad nimi ztrácí kontrolu, protože se nacházejí mimo stanovené hranice oprávnění. Organizace nyní nemůže vědět, jak dlouho jsou data uložena, kdo k nim má přístup nebo jak je třetí strana používá. To, co začalo jako rychlé zvýšení produktivity, se změnilo v incident úniku dat. Tento scénář odráží potenciální interní riziko, pokud zaměstnanec s dobrými úmysly sdílí citlivá data s neschváleným nástrojem s AI, čímž v organizaci vzniká nedostatek v zabezpečení.

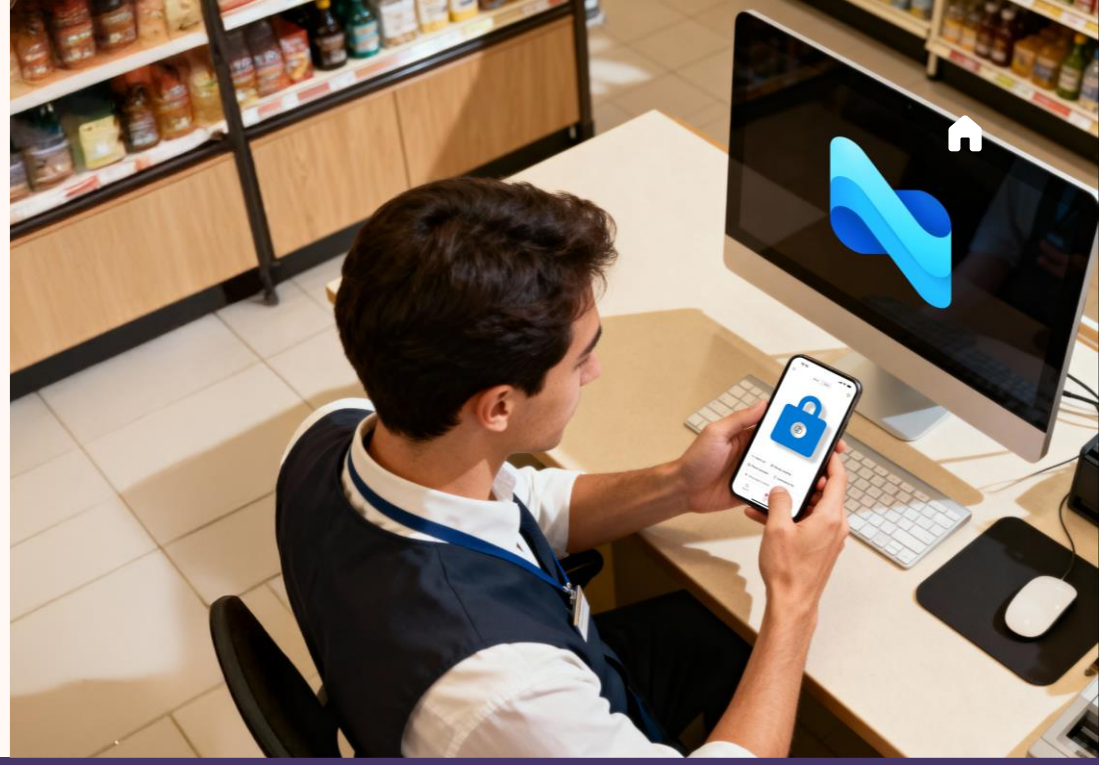
Zmírnění rizik prostřednictvím Microsoft 365 E3:

Microsoft 365 E3 zahrnuje několik funkcí a možností, které by mohly tomuto výsledku zabránit. **Microsoft Purview Information Protection Plan 1** umožňuje zavést popisky citlivosti a šifrování pro dokumenty, jako jsou plán produktu a finanční projektové dokumenty. Pokud by tyto dokumenty byly označeny popiskem citlivosti, například *Důvěrné*, a zašifrovány, přístup k nim by byl umožněn pouze autorizovaným uživatelům. Navíc **Cloud App Discovery** může pomoci identifikovat používané cloudové aplikace s generativní AI (z mnoha aplikací v katalogu cloudových aplikací) a zjistit, kteří uživatelé je využívají a jak často. IT tým mohl odhalit, že zaměstnanci používají tento konkrétní nástroj s AI, a podniknout kroky k omezení jeho používání pomocí **Microsoft Defenderu for Endpoint P1** nebo nabídnout oficiálně schválenou alternativu. Microsoft 365 E3 poskytuje nástroje a funkce, které organizacím pomáhají zlepšit přehled a zmírnit rizika.

2. ukázkový scénář[4]

Manažer maloobchodní prodejny používá AI k sestavení rozvrhů zaměstnanců a poznámek k pracovním výkonům

Manažer prodejny ve velkém maloobchodním řetězci je zahlcen úlohami správy a objeví bezplatnou pracovní aplikaci využívající AI, která slibuje pomoc s plánováním a dokumentací. Aby ušetřil čas, nahraje do nástroje s AI tabulku obsahující jména zaměstnanců, telefonní čísla, hodinové mzdy, preference dostupnosti a poznámky k nedávným pracovním výkonům. Požádá AI aplikaci, aby vytvořila optimalizovaný pracovní plán a pomohla navrhnout souhrny hodnocení výkonu pro nadcházející individuální pohovory.



Potenciální riziko:

Nahráním těchto údajů o zaměstnancích do neprověřené AI aplikace manažer zpřístupnil citlivé osobní údaje svých zaměstnanců systému třetí strany, nad kterým společnost nemá žádnou kontrolu ani dohled. To by mohlo vést k potenciálnímu narušení soukromí a problémům s dodržováním pracovního práva. Personální a IT oddělení společnosti nemají přehled o tom, kde jsou nyní data zaměstnanců uložena, jak dlouho jsou uchovávána ani kdo k nim může mít přístup. To, co začalo jako snaha o větší efektivitu, vedlo k vážným právním problémům, narušení soukromí a ztrátě důvěry zaměstnanců.

Zmírnění rizik prostřednictvím Microsoft 365 E3:

Funkce pro správu zařízení a aplikací v Microsoft 365 E3 mohou v takových pracovních scénářích pomoci zmírnit rizika. S **Microsoft Intune P1** může IT tým prodejce vynucovat zásady ochrany aplikací, které umožňují uplatňovat pravidla pro aplikace přistupující k pracovním datům, například omezit kopírování a vkládání a přenos dat do nespravovaných aplikací. Pokud prodejce vytvoří zásady podmíněného přístupu prostřednictvím **Microsoft Entra ID P1**, může zablokovat pokusy o přihlášení k podnikovým účtům z nespravovaných aplikací nebo zařízení. V tomto scénáři, pokud telefon manažera není v souladu s předpisy nebo aplikace není spravovaná, tyto zásady mohou pomoci zabránit přístupu k citlivým firemním souborům a jejich nahrání do stínové AI aplikace.

STĚŽEJNÍ POZNATEK: V obou scénářích byl záměr zaměstnanců pozitivní – zvýšit efektivitu práce pomocí AI. Výsledek však může být negativní, pokud nejsou nastaveny řádné mantinely a zásady. Tyto příklady zdůrazňují, proč může zavádění AI bez ochranných opatření přinést organizacím nová rizika navíc. Cílem není odrazovat od používání AI, ale umožnit její odpovědné využívání. Následující část se zabývá základními funkcemi, které je třeba zvážit při hodnocení řešení, jež mohou zvýšit produktivitu, a funkcemi Microsoft 365 E3, které organizacím umožňují nastavit ochranná opatření pomáhající uchovávat citlivá data ve schválených, zabezpečených kanálech.

Budování bezpečného základu připraveného na AI s Microsoft 365 E3

Je vaše organizace připravena škálovat AI? Projděte si kontrolní seznam níže a zjistěte, jak vám Microsoft 365 E3 může pomoci.

S tím, jak se zavádění AI zrychluje, je stále důležitější hodnotit stav zabezpečení organizace a odhalit případné nedostatky před rozšířením AI. Microsoft 365 E3 je navržen jako základ pro produktivitu a zabezpečení připravený na AI – kombinuje širokou škálu nástrojů pro identitu, zabezpečení, dodržování předpisů a správu, které ve vzájemné spolupráci umožňují škálovat zavedení AI s jistotou.

Použijte tento kontrolní seznam jako výchozí bod pro zjištění aktuálního stavu organizace. Pokud některé položky ještě nejsou plně implementovány, mohla by být vaše organizace vystavena zbytečnému riziku.

Prosazujte silné zásady pro správu identit a přístupu, jako jsou vícefaktorové ověřování (MFA) a podmíněný přístup.

Microsoft 365 E3 zahrnuje službu **Microsoft Entra ID P1**, která umožňuje prosazovat robustní správu identit a přístupu jak v cloudových, tak v místních prostředích. Řešení jako MFA a zásady podmíněného přístupu ověřují každé přihlášení a omezují, nebo povolují přístup na základě kritérií, jako je role uživatele, stav zařízení a poloha, což pomáhá předcházet neoprávněnému přístupu a nadměrnému sdílení dat. Můžete například omezit přístup k AI aplikacím na konkrétní skupiny zaměstnanců a vyžadovat vícefaktorové ověřování pro přihlášení, čímž se sníží riziko napadení účtu. Zásady podmíněného přístupu navíc chrání citlivá data tím, že zabrání zaměstnancům v přístupu k neschváleným aplikacím pomocí firemních přihlašovacích údajů, a sdílená zařízení mohou vynucovat pravidla odhlášení, která chrání před neoprávněným přístupem k relaci.

Zajistěte bezpečnou spolupráci napříč spravovanými koncovými body a zařízeními.

Microsoft 365 E3 poskytuje inteligentní zabezpečení koncových bodů prostřednictvím řešení, jako jsou **Intune P1, Defender for Endpoint P1 a Windows E3**. Tyto nástroje pomáhají spravovat počítače, mobilní zařízení a aplikace a zvyšovat jejich zabezpečení. Organizace můžou vynucovat filtrování webu a blokovat nebezpečné stránky (včetně neschválených nástrojů s AI) a udržovat zařízení v aktualizovaném stavu pomocí oprav zabezpečení prostřednictvím nástrojů **Windows Autopatch a Autopilot**. Tyto kontrolní mechanismy pomáhají udržovat zařízení v dobrém stavu, spravovaná a aktuální pomocí oprav zabezpečení, čímž zmenšují potenciální oblast útoku. Sjednocená správa koncových bodů a zařízení umožňuje organizacím zajistit bezpečnost pracovních zařízení a zachovávat dodržování předpisů v aplikacích, ať už zaměstnanci používají vlastní zařízení, nebo ta firemní.

Chraňte data pomocí funkcí, jako jsou popisky citlivosti a zásady ochrany před únikem informací.

Microsoft 365 E3 nabízí klíčové funkce **Purview** – popisky citlivosti, šifrování a ochranu před únikem informací (DLP) – pro ochranu citlivých informací v dokumentech a e-mailech. Jakmile jsou zásady pro popisky publikovány, mohou zaměstnanci klasifikovat soubory obsahující finanční údaje, osobní údaje nebo duševní vlastnictví (například pomocí popisku citlivosti „Důvěrné“), přičemž se na ně automaticky použije šifrování a řízení přístupu. Zásady ochrany před únikem informací (DLP) mohou detekovat a omezit neoprávněné sdílení napříč službami **Exchange Online a Microsoft Office SharePoint Online / OneDrive pro firmy**. I při používání **Microsoft 365 Copilota** zůstávají tyto ochrany v platnosti: Copilot respektuje nejvyšší popisek citlivosti a brání uživatelům bez oprávnění v přístupu ke chráněnému obsahu nebo jeho analýzám.

Získejte přehled o používání neschválených nástrojů s AI a zavádějte informovaná opatření.

Microsoft 365 E3 zahrnuje službu **Cloud App Discovery**, která vám pomůže zjistit, jaké AI aplikace jsou používány (z těch, které jsou zahrnuty v katalogu cloudových aplikací), kým a s jakými souvisejícími skóre rizika, abyste mohli na základě těchto informací rozhodnout o dalším postupu. Pokud je vyhodnocena jako příliš nebezpečná, může IT použít **Defender for Endpoint P1** k omezení přístupu uživatelů na danou adresu URL na spravovaných zařízeních s Windows 11. Pokud například zjistíte, že 100 uživatelů používá AI generátor obrázků, který dosud nezkontrolovalo nebo neschválilo IT oddělení, může IT tento nástroj prověřit podle standardů zabezpečení a dodržování předpisů v organizaci. Pokud bude považován za nebezpečný, může IT doporučit oficiální alternativu. Tyto funkce umožňují omezit rizika stínové AI a informovaně se rozhodovat o využívání AI tak, jak je to vhodné pro organizaci.

Poskytujte schválené aplikace AI, jako je Microsoft 365 Copilot.

Poskytování schválených aplikací AI přináší významnou hodnotu tím, že zaměstnancům umožňuje přístup k výkonným, schváleným nástrojům, které splňují standardy zabezpečení a dodržování předpisů v organizaci. Například místo toho, aby se zaměstnanci obraceli na neprověřené AI generátory obrázků nebo chatboty, může IT nabídnout schválené alternativy, jako je **Microsoft 365 Copilot,** které jsou monitorovány, podporovány a integrovány do stávajících zásad společnosti. **Microsoft 365 Copilot** nabízí bezpečné řešení AI na podnikové úrovni, které je plně integrováno do sady produktivity Microsoft 365. **Copilot** umožňuje zaměstnancům pracovat chytřeji, automatizovat rutinní úkoly a generovat poznatky – to vše při respektování zásad ochrany identit a dat. Tento přístup omezuje stínové IT, pomáhá omezit úniky dat a poskytuje organizacím přehled a kontrolu nad tím, jak je AI využívána.

Tyto funkce nefungují izolovaně – vzájemně se posilují jako integrovaná, vícevrstvá obrana. Zásady ochrany identit, zařízení a dat společně pomáhají zmírňovat hrozby. Když bezpečnostní týmy vědí, že jsou zavedena opatření jako tato, může se zabezpečení stát podporovatelem inovací namísto překážky.

Microsoft 365 E3 umožňuje nastavit správná ochranná opatření, aby organizace mohla inovovat s AI, aniž by bylo ohroženo zabezpečení.

Pokračování na cestě k zavedení AI

Každá organizace se pokouší zjistit, jak může AI nejlépe sloužit jejím cílům. Příslib je lákavý – ale zavedení AI musí jít ruku v ruce s robustní ochranou. Díky Microsoft 365 E3 si nemusíte vybírat jedno, nebo druhé. Získáte výkonnou sadu, která posiluje zabezpečení a dodržování předpisů, což umožňuje využívat AI s důvěrou.

Posuďte svou připravenost v oblasti zabezpečení AI.

Microsoft nabízí **Posouzení zabezpečení pro AI**[3]. Toto online posouzení (na adrese security-for-ai-assessment.microsoft.com) nabízí doporučení pro zvýšení zabezpečení AI na základě informací, které poskytnete. Pomáhá posoudit aktuální úroveň zabezpečení AI v organizaci podle čtyř zásadních pilířů "**příprava**, **zjišťování**, **ochrana** a **správa"** a také poskytuje konkrétní doporučení k dalším krokům.

Zjistěte více a kontaktujte Microsoft.

Prozkoumejte podrobněji možnosti Microsoft 365 E3 a zjistěte, jak vám mohou pomoci s jistotou zavést AI. www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab. Můžete se také obrátit na tým správy účtu Microsoft nebo na svého partnera.

1. Index pracovních trendů: výroční zpráva, 2025: Rok vzniku průkopnických firem Microsoft, Inc., duben 2025. Společnost Microsoft analyzovala data z průzkumu mezi 31 000 zaměstnanci na plný úvazek nebo osobami samostatně výdělečně činnými, kteří pracují se znalostmi v 31 zemích, a to v období od 6. února 2025 do 24. března 2025, z trendů na pracovním trhu LinkedInu a bilionů signálů o produktivitě z Microsoftu 365.
2. Second Annual Generative AI Study: Business Rewards vs. Security Risks, iSMG, Inc., únor 2025 – na základě průzkumu mezi více než 360 odborníky v oblasti obchodu a kybernetického zabezpečení, vypracováno ve 3. čtvrtletí 2024.
3. Posouzení zabezpečení pro AI: security-for-ai-assessment.microsoft.com/ Přesnost výsledků závisí na přesnosti vašeho zadání. Zpráva je pouze informativní a nezaručuje výkonnost ani výsledky. Neměla by být vykládána jako závazek Microsoftu. Skutečné výsledky se mohou lišit v závislosti na faktorech, jako je lokalita, způsob nákupu a využití. Microsoft neposkytuje žádné výslovné ani odvozené záruky týkající se obsahu této zprávy nebo webu.
4. Prezentované scénáře jsou fiktivní a jsou pouze ilustrativní.