

# Předcházení hrozbám: malé a středně velké podniky se zaměřují na počítače s AI

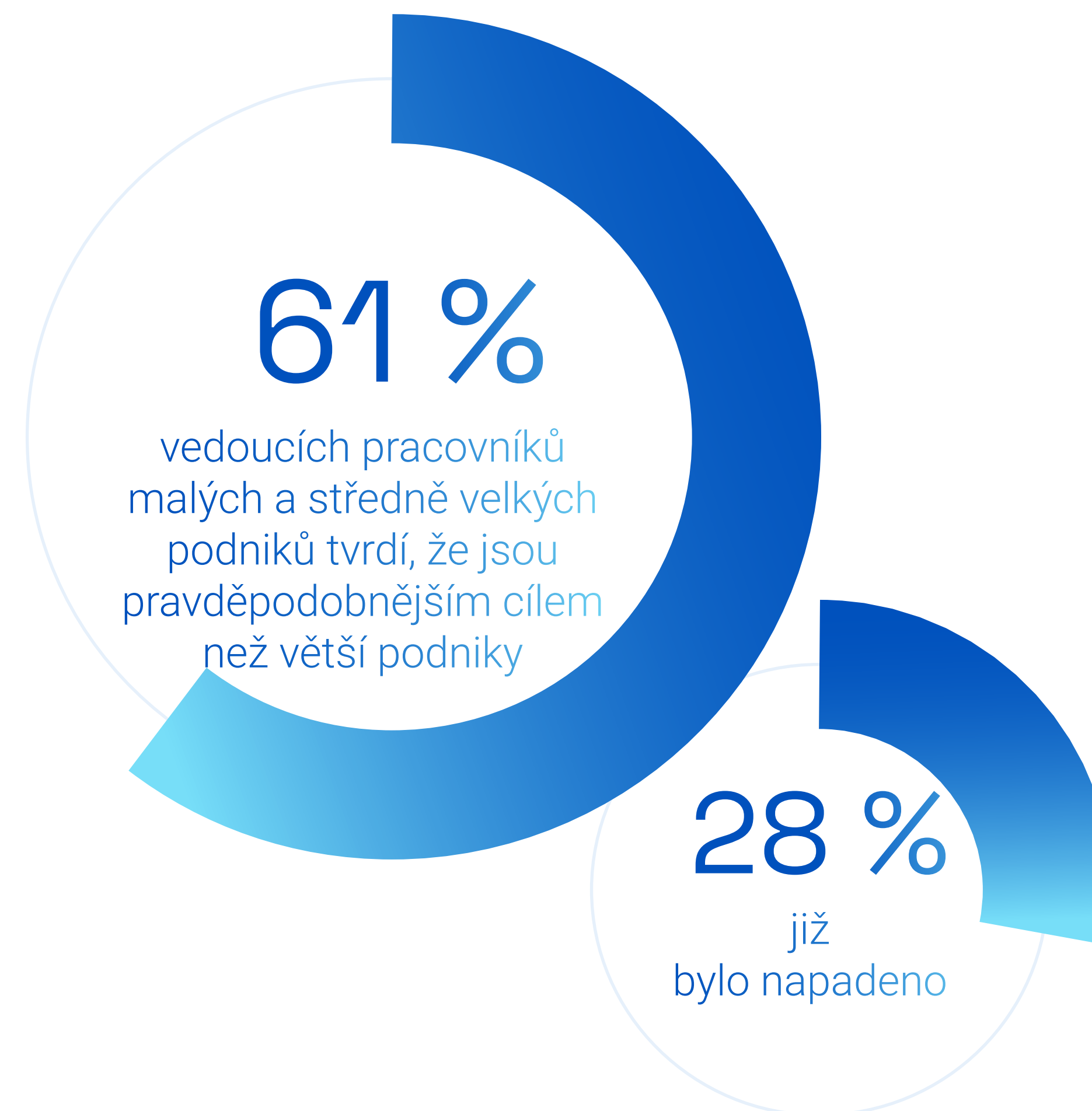
Zůstat v bezpečí znamená zůstat proaktivní –  
a používat správné technologie.



Kybernetická bezpečnost se oficiálně stala problémem všech. A pro malé a středně velké podniky (SMB) je tato hrozba osobní. Podle **zprávy společnosti ASUS o budoucnosti malých a středně velkých podniků z roku 2025**, se téměř **61 % vedoucích pracovníků malých a středně velkých podniků domnívá, že je pravděpodobnější, že se stanou terčem kybernetických útoků, než větší podniky.** A protože více než čtvrtina z nich uvedla, že jejich podnik již byl napaden, není toto přesvědčení jen paranoiou.

Přestože si mnozí toto riziko uvědomují, méně z nich se cítí být plně připraveni. **Pouze 1 z 5 vedoucích pracovníků malých a středně velkých tvrdí, že se cítí „velmi bezpečně“**, zatímco více než 25 % se cítí neutrálně nebo se necítí bezpečně. Tento rozdíl ve vnímání je výmluvný: ukazuje na skupinu, která sice chápe, že kybernetická bezpečnost je důležitá, ale stále nemá důvěru ve svou obranu. Problémem často není informovanost. Jde o to vědět, co dělat dále.

Povzbudivé je, že malé a středně velké podniky nezažalují. 85 % respondentů se v oblasti kybernetické obrany považuje za velmi proaktivní nebo spíše proaktivní. To zahrnuje **aktualizaci softwaru, monitorování systémů a školení zaměstnanců.** Pouze 40 % z nich však tvrdí, že jsou „velmi“ proaktivní, což ukazuje na příležitost přejít od reaktivních řešení k integrované ochraně zaměřené na budoucnost.





**41 %**   
využívá AI ke zvýšení bezpečnosti

# Předcházení útokům začíná chytřejšími nástroji

Právě v této oblasti je AI důležitá. **41 % majitelů malých a středně velkých podniků uvádí jako hlavní výhodu technologií AI vyšší bezpečnost a zabezpečení proti selhání.** A není těžké pochopit proč. Od detekce neobvyklého chování až po automatizaci rychlé reakce – AI pomáhá malým a středně velkým podnikům dělat to, co tradiční bezpečnostní systémy nedokážou: být o krok napřed. **Vzhledem k tomu, že kybernetických útoků přibývá rychleji, než lidé dokáží reagovat, jsou inteligentní nástroje nejen užitečné, ale i nezbytné.**

Počítače s AI, jako je řada ASUS Expert P, tuto změnu symbolizují. Tyto počítače s AI

jsou vybaveny integrovanými funkcemi zabezpečení koncových bodů, které se vyvíjejí spolu s novými hrozbami. Pro malé a středně velké podniky, které nemají specializované IT týmy, může tento druh **integrované inteligence znamenat rozdíl mezi narušením a prevencí.** Přináší klid bez dalších složitostí a nákladů.

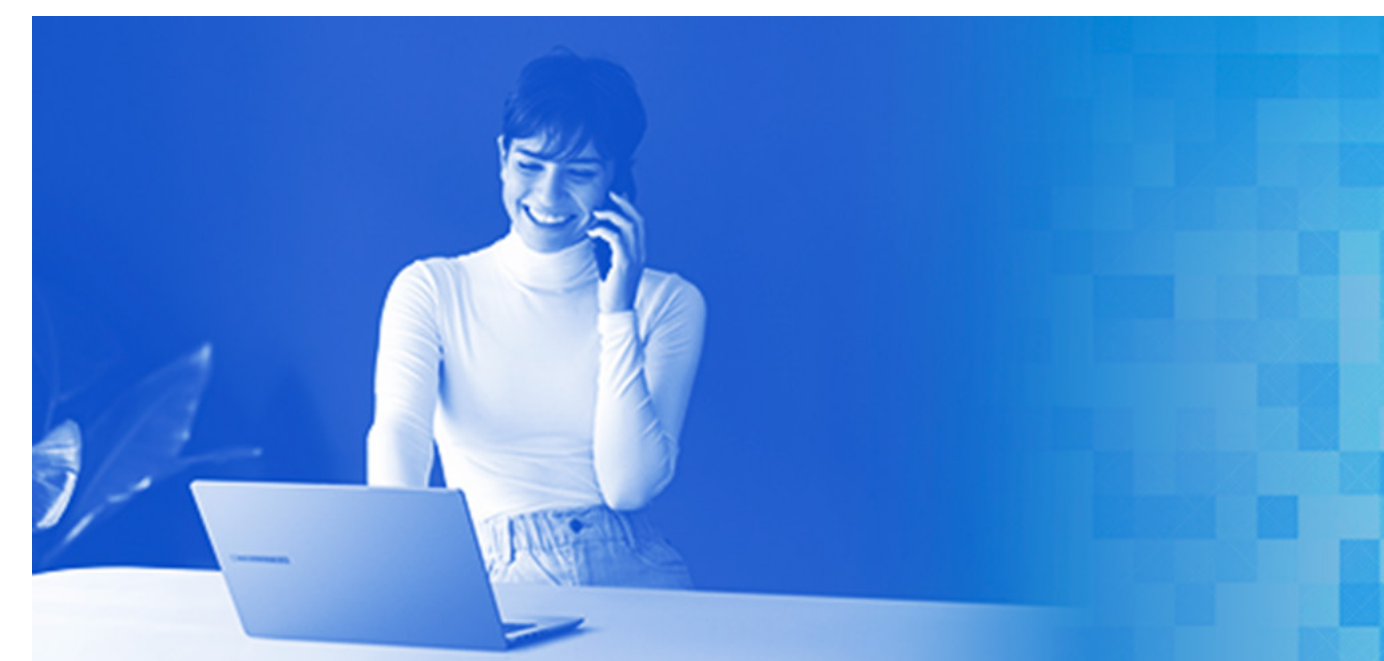


# Nejnebezpečnějším rizikem je podceňování rizika

Přesto ne všichni pociťují naléhavost situace. Přibližně **15 % vedoucích pracovníků malých a středně velkých podniků se domnívá, že je méně pravděpodobné, že se stanou terčem útoku, než velké podniky – což odhaluje riskantní falešný pocit bezpečí.** Dnešní kybernetické útoky však nejsou jen cílené; jsou automatizované, oportunistické a vždy hledají nejsnazší cestu. A pro nepřipravené podniky neznamena, že malý podnik je neviditelný. Znamená to, že jste zranitelní, pokud nejste připraveni.

Pro malé a středně velké podniky není cílem dokonalost. Je to odolnost. To znamená vytvořit kulturu kybernetické bezpečnosti, která prochází všemi vrstvami podniku, od lidí až po infrastrukturu. **Skutečná ochrana vyžaduje více než jen hesla a zásady, vyžaduje integrovanou ochranu na úrovni jednotlivých zařízení.**

A právě zde přichází na řadu ASUS ExpertGuardian. Toto **bezpečnostní řešení podnikové úrovně** určené pro zařízení ASUS ExpertBook a ExpertCenter, poskytuje víceúrovňovou ochranu od hardwaru po software. Zahrnuje fyzicky izolovaný zabezpečený procesor, který **chrání systém BIOS a firmware před neoprávněným zásahem**, automatické obnovení systému BIOS, zámky přístupu k USB a 5 let průběžných aktualizací zabezpečení firmwaru, které jsou v souladu s předními směrnicemi NIST. Podnikům bez velkých IT týmů poskytuje ExpertGuardian **obranu v reálném čase, integrované funkce samoopravy a vzdálené správy**, které pomáhají předcházet hrozbám, detekovat je a automaticky na ně reagovat. Jakmile totiž dojde k narušení, nejsou ohrožena jen vaše data, ale i důvěra zákazníků, vaše pověst a kontinuita vašeho podnikání. A pro většinu malých a středně velkých podniků je jejich obnovení obtížnější než obnovení dat.



Čelíte rostoucím kybernetickým rizikům?  
Zjistěte, jak mohou být počítače ASUS s AI  
vaší základní obrannou linií.

Spojte se s námi ještě dnes a domluvte si  
schůzku, na které probereme jedinečné  
potřeby vaší organizace.