

OPERAČNÍ PROGRAM  
TECHNOLOGIE A APLIKACE  
PRO KONKURENCESCHOPNOST



MINISTERSTVO  
PRŮMYSLU A OBCHODU

## Digitální podnik - Digitální technologie



10. Října 2025



KAM KRÁČÍ DIGITÁLNÍ SÍŤ  
PLZEŇ 2025



Spolufinancováno  
Evropskou unií

# Digitální podnik – Digitální technologie – výzva I.

**Východiska:** Hlavním cílem je prostřednictvím zvýšení digitální úrovně a akcelerace digitální transformace usnadnit proces přechodu MSP (**včetně služeb**) na plné využití rychle se rozvíjející digitální ekonomiky a společnosti, a tím zajistit, resp. zvýšit jejich konkurenceschopnost, a to prostřednictvím komplexních investic ve smyslu zavádění pokročilých technologií, robotizace a automatizace a zavedení principů průmyslu 4.0.

**Druh výzvy:** Kolová

**Model hodnocení:** Jednokolový

**Datum vyhlášení Výzvy:** 26. září 2025 (posun o jeden týden oproti původnímu HMG)

**Datum zahájení příjmu žádostí o podporu:** 20. října 2025

**Datum ukončení příjmu žádostí o podporu:** 18. února 2026

**Ukončení fyzické realizace projektu:** 31. ledna 2028

**Alokace výzvy:** 1 mld. (Řídící orgán může příjem žádostí o podporu ukončit poté, co finanční objem v podaných žádostech o podporu dosáhne 100 % výše alokace výzvy, nejdříve však 4. 11. 2025.)

**Cílová skupina:** MSP s dvouletou historií

**Výše podpory:** Celkové způsobilé výdaje (dále také „CZV“) na projekt musí být minimálně ve výši 2,5 mil. Kč a maximálně do výše 100 mil. Kč.

# Digitální podnik – Digitální technologie – výzva I.

**Míra podpory:** dle Regionální mapy, podpora směřuje jen do území přechodových regionů České republiky (tj.: Regiony NUTS 2 Střední Čechy, Jihozápad a Jihovýchod)



Region	Malý podnik	Střední podnik
<b>Střední Čechy</b> – Rakovník, Kladno, Mělník	45 %	35 %
<b>Střední Čechy</b> – Mladá Boleslav, Beroun, Praha-západ, Praha-východ, Nymburk, Kolín, Příbram, Benešov, Kutná Hora	35 %	25 %
<b>Jihozápad</b> – Plzeň-sever, Tachov	45 %	35 %
<b>Jihozápad</b> – Rokycany, Plzeň, Plzeň-Jih, Domažlice, Klatovy, Písek, Tábor, Strakonice, České Budějovice, Jindřichův Hradec, Prachatice, Český Krumlov	35 %	25 %
<b>Jihovýchod</b>	35 %	25 %

**Bonifikace znevýhodněných regionů:** ORP v HSOÚ a/nebo na územích s vyšší než průměrnou mírou nezaměstnanosti

# Model hodnocení k výzvě Digitální podnik – Digitální technologie – výzva I.

Kritéria pro věcné hodnocení jsou rozdělena do pěti základních kategorií

**A Vylučovací kritéria (ANO x NE)**

**B Kvalita a strategické zaměření SW**

**(hodnotící kritérium, max. 29 bodů)**

**C Kvalita a strategické zaměření HW**

**(hodnotící kritérium, max. 27 bodů)**

**D Kvalita a strategické zaměření SLU**

**(hodnotící kritérium, max. 14 bodů)**

**E Výrobní technologie**

**(hodnotící kritérium, max. 30 bodů)**

**F Bonifikace znevýhodněných regionů**

**(hodnotící kritérium, max. 3 body)**

Na rozdíl od I. výzvy Digitální podnik – Technologie 4.0 – výzva I., nebude ve věcném hodnocení vyžadováno splnění minimálního počtu bodů pro jednotlivé kategorie kritérií, ale počítá se jen celkový počet bodů dohromady.

Je nutné splnění všech kritérií kategorie A a zároveň součet bodů za kategorie B, C, D a E musí být **minimálně 50**.

Kritérium E se zaměřuje na cenu výrobních strojů zahrnutých do projektu. Body se přidělují podle toho, jak vysoká je předpokládaná cena těchto strojů. Projekty, které výrobní stroje vůbec neobsahují, nebo je mají jen v menší hodnotě, získávají v tomto kritériu bodovou výhodu.

Obsahově se jednotlivá kritéria věcného hodnocení oproti výzvě Digitální podnik – Technologie 4.0 a Digitální podnik – digitální podnik – výzva I. OP TAK nemění.

# Model hodnocení k výzvě **Digitální podnik – Digitální technologie – výzva I.**

**A Vylučovací kritéria (ANO x NE):** Bez rozdílů oproti předchozím výzvám.

**B Kvalita a strategické zaměření SW (29 b.):** Digitalizace procesů klíčových vnitropodnikových procesů, sofistikované řízení skladu, vývoje a technických dokumentací, komplexní plánování v kapacitách, řízení životního cyklu výrobků; online flexibilita výroby, monitoring prvků systému a využití průlomových technologií.

**C Kvalita a strategické zaměření HW (27 b.):** Dohled a automatizované řízení procesů, síťová infrastruktura, správa osob a přístupů, monitoring, vzdálený přístup, 24/7 prodejny a kybernetické zabezpečení; robotizace manipulace a skladování.

# Model hodnocení k výzvě **Digitální podnik – Digitální technologie – výzva I.**

**D Kvalita a strategické zaměření SLU (14 b.):** Pronájem výpočetního výkonu nebo specializovaných služeb, vytvoření digitálního dvojčete, služby vzdálené správy kybernetického zabezpečení a služby expertní analýzy úrovně zajištění kyberbezpečnosti včetně návrhu a implementace nápravných prvků a opatření, nebo certifikace zaměstnanců.

**E Výrobní technologie (30 b.):** Předpokládaná cena výrobních technologií dle výše nejnižších doložených indikativních nabídek do: 0,- Kč = 30 b. 25 000 000,- Kč = 15 b.

**F Bonifikace znevýhodněných regionů (3 b.)**

# Detail na kyberbezpečnost

## Software

Monitoring síťových zařízení: systém, který sbírá a vyhodnocuje informace o stavu zařízení (např. routery, switche, tiskárny, servery) a umožňuje jejich centrální dohled.

## Hardware

1. Prvky kybernetické bezpečnosti, zařízení, která chrání firemní síť a pomáhají odhalovat nebo zastavit útoky:

- Firewall – „brána“ sítě, která filtruje přístup dovnitř i ven podle nastavených pravidel.
- IDS/IPS – systém, který sleduje síťový provoz, rozpozná škodlivou aktivitu a v případě potřeby ji zablokuje.
- Sběr a analýza dat o síťovém provozu – tzv. sondy, které ukládají informace o provozu v síti (kdo, kam a kdy se připojuje). Tyto záznamy lze využít pro vyšetření incidentů nebo pro odhalování neznámých hrozeb.

2. Správa zranitelností: zařízení, které pravidelně kontroluje IT systémy a sítě, vyhledává slabá místa a vyhodnocuje jejich závažnost, aby se předešlo útokům.

## Služby

1. Kyberbezpečnost, odborná pomoc a dlouhodobá péče o kybernetickou bezpečnost:

- Outsourcing kyberbezpečnosti – zajištění provozu, správy a testování bezpečnosti sítě. Zahrnuje např. penetrační testy, audit, monitoring událostí (SOC), školení zaměstnanců, řešení incidentů a správu aktualizací.

2. Analýza a implementace prvků kybernetické bezpečnosti:

- Spolupráce s expertem, který posoudí aktuální stav zabezpečení firmy, doporučí vhodná řešení a pomůže s jejich zavedením.



MINISTERSTVO  
PRŮMYSLU A OBCHODU

DĚKUJEME  
ZA POZORNOST

