

podporuje



60__dB

Touha prosperovat – část 4: Shrnutí části studie

Kybernetická bezpečnost českých
mikro- a malých podniků
v roce 2025

Zpráva 60 Decibels
pro Mastercard Strive
v Česku

Úvod

S tím, jak české mikro- a malé podniky procházejí digitalizací, se kybernetická bezpečnost stává klíčovým tématem – výzvou i příležitostí zároveň. Tento souhrnný výstup z posledního ze čtyř Barometrů českého podnikatelského prostředí přináší pohled na to, jak tyto podniky vnímají kybernetická rizika, jaké mají zkušenosti s incidenty a jak (ne)investují do ochrany. Dotazníkové šetření provedené mezi 613 mikro-

a malými podniky v Česku v období od prosince 2024 do ledna 2025 odhaluje rostoucí povědomí, přetrvávající podinvestovanost a rozdíly mezi regiony i mezi podniky vedenými muži a ženami. Studie rovněž upozorňuje na hlavní překážky a potřeby, které je třeba řešit, aby se zlepšila kybernetická odolnost tohoto zásadního segmentu ekonomiky.

Hlavní zjištění

- 1. Kybernetická bezpečnost je vnímána jako důležitá – ale ne všemi a ne prioritně.** Dvě třetiny podniků považují kybernetickou bezpečnost za důležitou – 33 % ji označuje za „velmi důležitou“ a dalších 36 % za „spíše důležitou“. Nejčastěji zmiňovanými obavami jsou úniky dat (přes 50 %) a krádež identity (44 %). Zároveň však 10 % podnikatelů uvedlo, že se kybernetických hrozeb vůbec neobává, což poukazuje na významný deficit v povědomí.
- 2. Zkušenost s kybernetickým incidentem zvyšuje ochotu investovat.** Téměř třetina podniků má zkušenost s kybernetickým incidentem. Tyto podniky jsou výrazně ochotnější investovat do ochranných opatření – 84 % oproti 76 % u těch, které incident nezažily. Mikro- a malé podniky čelily útokům častěji než podniky bez zaměstnanců (34 % vs. 28 %).
- 3. Většina podniků přijímá základní bezpečnostní opatření – ale jen málo z nich jde dál.** Antivirový software používá necelých 70 % podniků, zhruba 60 % pravidelně aktualizuje software a používá dvoufaktorové ověření. Méně než polovina (49 %) však využívá firewally a ještě méně šifruje data (34 %) nebo školí zaměstnance v oblasti kybernetické bezpečnosti (42 %).
- 4. Investice jsou omezené kvůli vysokým nákladům, nedostatku dovedností a nedostatečnému přesvědčení o významu kybernetické bezpečnosti.** Čtyři z deseti podniků jsou ochotné investovat do kybernetické bezpečnosti méně než 500 Kč měsíčně. Mezi hlavní překážky patří náklady (31 %) a nedostatek odborných znalostí (26 %), dále pak nízká priorita tématu (27 %) a nedostatek času (22 %). Každý desátý podnikatel přiznává, že vůbec nechápe přínos kybernetické bezpečnosti.



podporuje



strive



care®

60__dB

- 5. Gender majitele a velikost podniku ovlivňují ochotu investovat i míru obav.** Podniky vedené ženami se více obávají krádeže identity (47 % oproti 43 % u mužů), zatímco muži se více obávají malwaru (38 % vs. 28 % u žen). Částku menší než 500 Kč měsíčně je ochotná investovat polovina žen (oproti 38 % mužů). Mikro- a malé podniky vykazují vyšší míru ohrožení a mírně proaktivnější přístup než podniky bez zaměstnanců.
- 6. Podnikatelé požadují dostupné nástroje, odborné poradenství a školení.** Na otázku, co by pomohlo zlepšit jejich kybernetickou bezpečnost v praxi, 40 % podnikatelů uvedlo cenově dostupné nástroje, 35 % zmínilo školení a 31 % přístup k odbornému poradenství. Ženy častěji než muži požadují školení a zvyšování povědomí, zatímco menší podniky upřednostňují cenovou dostupnost.
- 7. Regionální rozdíly ukazují nerovnoměrnou připravenost v oblasti kybernetické bezpečnosti.** Podniky v Praze vykazují nejvyšší míru povědomí i ochoty investovat do kybernetické bezpečnosti – přes 70 % z nich považuje kyberbezpečnost za prioritu a 40 % je ochotno investovat více než 500 Kč měsíčně. Naproti tomu severozápadní, severovýchodní a střední Čechy¹ vykazují nižší úroveň připravenosti. Ve středních Čechách například 21 % podniků nepovažuje kybernetickou bezpečnost za důležitou a 19 % jí nerozumí.
- 8. Sektorové rozdíly odrážejí míru rizika.** Podniky ve zdravotnictví, financích a logistice vykazují vyšší obavy i ochotu investovat. Maloobchod, pohostinství a stavebnictví, které často operují s nižšími maržemi a méně citlivými daty, mají tendenci kyberbezpečnost odsouvat na vedlejší kolej.

Doporučení

Pro zlepšení připravenosti českých mikro- a malých podniků v oblasti kybernetické bezpečnosti, zejména těch s omezenými zdroji, doporučujeme následující kroky:

- 1. Zajistit přístup k cenově dostupným nástrojům kybernetické bezpečnosti.** Mnoho podnikatelů vnímá náklady jako hlavní překážku přijetí účinnějších bezpečnostních opatření. Řešením mohou být dotace, zvýhodněné balíčky služeb nebo bezplatné úvodní nástroje určené podnikům s nízkými rozpočty.
- 2. Rozšířit praktická školení a programy digitální hygieny.** Vzhledem k tomu, že 35 % podniků projevilo zájem o školení, je třeba vytvořit srozumitelné a prakticky zaměřené programy, které pomohou podnikatelům porozumět základním principům kybernetické bezpečnosti a aplikovat je v praxi. Školení by měla být přizpůsobena technickým dovednostem podnikatelů.
- 3. Zajistit dostupné odborné poradenství.** Téměř třetina podnikatelů by uvítala přístup k cenově dostupným poradcům nebo konzultantům v oblasti kybernetické bezpečnosti. Tyto služby mohou být zajištěny prostřednictvím partnerství mezi veřejným a soukromým sektorem nebo přes místní hospodářské komory.
- 4. Zaměřit cílenou osvětu na regiony a odvětví s nízkou mírou povědomí o kybernetické bezpečnosti.** Podnikatelé v málo digitalizovaných odvětvích, jako je stavebnictví nebo pohostinství, a v regionech, jako jsou severozápadní Čechy, kde je digitální zapojení nižší, často kyberbezpečnost odsouvají na okraj. Cílené informační kampaně a případové studie z praxe mohou zvýšit vnímání naléhavosti a zájem o téma.
- 5. Zohlednit genderové rozdíly v investicích a přístupu ke kybernetické bezpečnosti.** Podniky vedené ženami investují do kybernetické bezpečnosti méně a často se cítí méně informované. Školení a podpůrné programy by měly být uzpůsobeny jejich potřebám, například formou flexibilních formátů nebo skupinového učení mezi podnikateli.

¹Regiony soudržnosti CZ-NUTS 2 podle normalizované klasifikace územních celků v Česku pro potřeby Eurostatu a ČSÚ https://csu.gov.cz/klasifikace_uzemnich_statistickych_jednotek_-cz_nuts-

- 6. Zařadit kybernetickou bezpečnost do širších strategií digitalizace.** Kybernetická bezpečnost by neměla být vnímána jako oddělené téma. Její propojení s dalšími oblastmi digitální transformace – například s e-commerce nebo účetnictvím – může přispět k širšímu a běžnějšímu uplatňování bezpečnostních opatření.
- 7. Využít stávající platformy a místní podnikatelské sítě.** Platformy jako Pro podnikavé mohou sloužit jako účinné nástroje pro šíření informací, nástrojů a podpory. Lokální sítě podnikatelů mohou navíc podpořit sdílení zkušeností a vzájemné učení, což je zvláště cenné pro podniky bez zaměstnanců.

Závěr

Kybernetická bezpečnost už není volitelná – je nezbytná pro každý mikro- a malý podnik v Česku. Spolu s digitalizací roste zranitelnost podniků vůči kybernetickým hrozbám, které mohou ohrozit jejich provoz, finance i důvěru zákazníků. Ačkoliv se povědomí zvyšuje, mezery ve znalostech, investicích i připravenosti přetrvávají – nejvíce u podniků bez zaměstnanců, podniků mimo Prahu a těch vedených ženami.

K zajištění jejich odolnosti je třeba cílená podpora – cenově dostupné nástroje, přístupná školení a regionálně přizpůsobené aktivity. Koordinovaným úsilím veřejného a soukromého sektoru lze zajistit, aby se kybernetická bezpečnost stala standardem – a nikoliv opomíjeným tématem – pro páteř české ekonomiky.

