12. Kybernetická bezpečnost

S rozšiřováním informačních a komunikačních technologií vzrůstá i riziko jejich napadení a zneužití získaných informací. Proto je důležité věnovat pozornost jejich zabezpečení. Kybernetická bezpečnost slouží k ochraně počítačových systémů, sítí, zařízení, programů a dat před digitálními útoky, poškozením, odcizením nebo neoprávněným přístupem. Cílem je zajistit, aby citlivé informace zůstaly chráněny a aby IT systémy fungovaly bez přerušení.

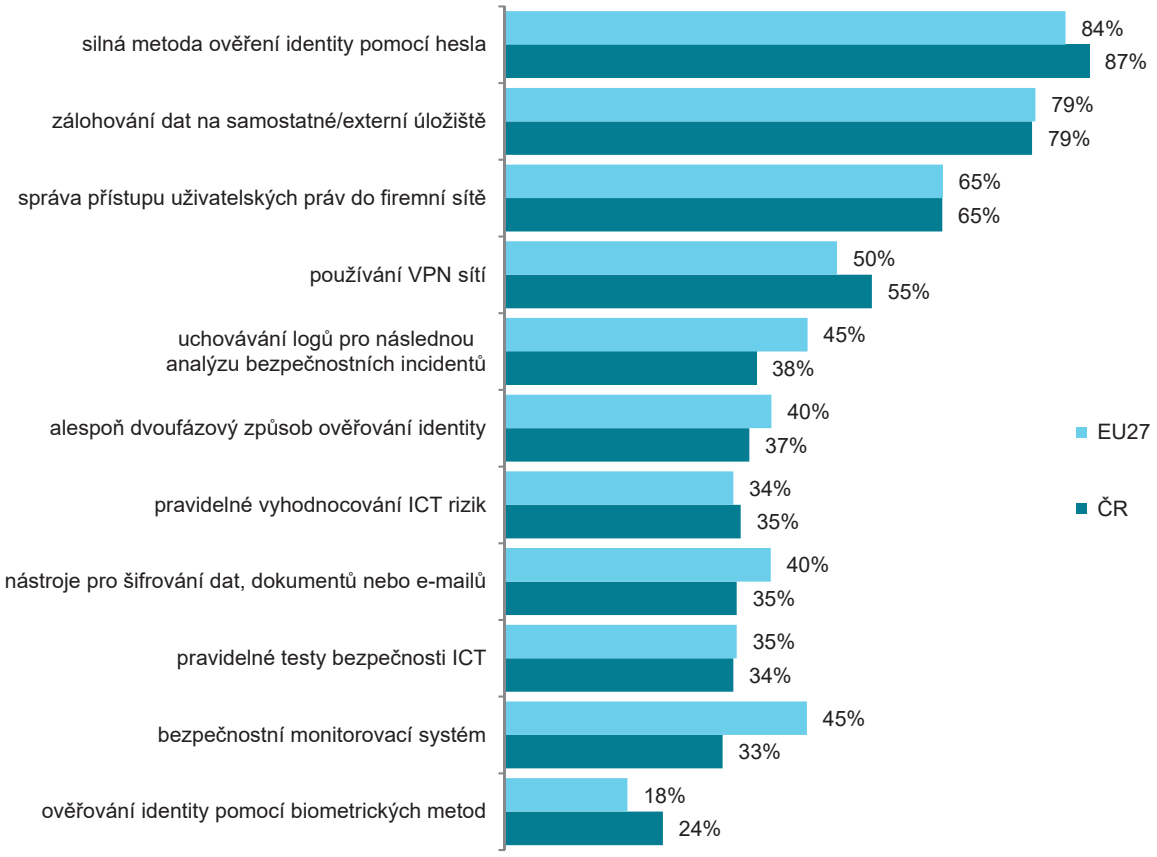
Hlavní zjištění

- Nejběžnějším opatřením k zajištění kybernetické bezpečnosti bylo v roce 2024 používání **silné metody ověření pomocí hesla** do počítače, sítě nebo aplikací. Používalo ho více než 87 % podniků u nás, téměř všechny velké (98 %). Druhým nejčastěji využívaným opatřením pak bylo **zálohování** firemních dat na samostatné nebo externí úložiště. To využívalo 79 % firem v ČR s více než 10 zaměstnanci, velkých firem bylo více než 95 %.
- Třetím nejčastěji využívaným bezpečnostním opatřením v roce 2024 byla **správa řízení přístupu uživatelů a zařízení** (uživatelských práv) **do podnikové sítě**. Toto opatření používalo průměrně 65 % podniků u nás. Jeho využívání se výrazně liší v závislosti na velikosti subjektů. Správu řízení přístupu používá 60 % malých firem, středně velkých subjektů je 86 % a velkých 97 %.
- Více než polovina firem v ČR (55 %) používá **virtuální privátní síť (VPN)**, která zprostředkovává zabezpečený vzdálený přístup z jakéhokoli místa do firemní počítačové sítě. I v tomto případě platí, že používání VPN se významně liší podle velikosti subjektů. Přístup přes internet pomocí VPN používá 96 % velkých firem, 79 % středně velkých a téměř polovina (48 %) malých.
- Každé z následujících šesti opatření k zajištění kybernetické bezpečnosti bylo v roce 2024 používáno více než třetinou firem. Jedná se o **uchovávání tzv. logů** (38 % podniků), pro následnou analýzu proběhlých bezpečnostních incidentů, **rozpoznávání identity uživatelů založené na alespoň dvoufázovém způsobu** (37 % podniků), tj. například pomocí znalosti hesla a dále díky jednorázovému vygenerovanému heslu či kódu zaslanému prostřednictvím speciální aplikace nebo pomocí SMS. 35 % podniků pravidelně **vyhodnocuje ICT rizika**, resp. pravděpodobnost výskytu bezpečnostních incidentů. 35 % podniků používalo nástroje pro **šifrování** dat, dokumentů nebo e-mailové komunikace. 34 % podniků provádí pravidelné **testy bezpečnosti ICT**. Třetina firem v ČR používala **bezpečnostní monitorovací systém**, který sleduje chování uživatelů a zařízení v síti a dokáže odhalit podezřelou aktivitu v ICT systémech.
- Nejméně využívanou metodou kybernetické bezpečnosti je **využívání biometrických metod** k rozpoznávání a ověřování uživatelů. V roce 2024 používalo tento způsob rozpoznávání a ověřování 24 % podniků v Česku.
- U všech výše popsaných opatření využívaných firmami k zajištění bezpečnosti ICT platí, že je nejvíce využívají velké podniky a nejméně malé firmy a z hlediska příslušnosti firem k odvětví jsou nejvíce uplatňovány podniky působícími v sekci CZ NACE J Informační a komunikační činnosti, tedy konkrétně v IT oboru, telekomunikacích a audiovizuálním sektoru.
- **Zajišťování povědomí o povinnostech zaměstnanců souvisejících s kybernetickou bezpečností** se ve firmách v ČR děje nejčastěji dobrovolným školením zaměstnancům, např. zveřejněním informací na intranetu. Tímto způsobem to provádí 53 % firem s deseti a více zaměstnanci. Dobrovolné školení využívá polovina malých firem, 61 % středně velkých a 75 % velkých subjektů.
- Dalších 28 % podniků seznamuje své zaměstnance s jejich povinnostmi souvisejícími s bezpečností ICT na **povinných kurzech nebo pomocí povinného prostudování** materiálů. Povinné školení zaměstnanců praktikuje více než 71 % velkých firem v ČR. Zajištění povědomí o povinnostech souvisejících s bezpečností ICT se dají zakotvit také např. do pracovní smlouvy. Tuto možnost využívá 32 % subjektů v ČR, 39 % středně velkých firem a 45 % velkých podniků.
- V naprosté většině podniků v zemích EU probíhá seznamování zaměstnanců s jejich povinnostmi souvisejícími s bezpečností ICT, stejně jako v podnicích v ČR, nejčastěji formou dobrovolného školení nebo např. informacemi zveřejněnými na intranetu. České podniky využívaly v roce 2024 dobrovolné školení zaměstnanců častěji (53 %), než v průměru v ostatních zemích Unie, průměr za EU27 činil 43 %. Povinné školení v oblasti bezpečnosti ICT pořádalo ve stejném roce 28 % podniků v ČR, průměr za EU

je v tomto případě 25 % podniků a ukotvení povinností souvisejících s bezpečností ICT ve smlouvě, např. v pracovní smlouvě, aplikuje 32 % podniků v ČR a v průměru EU je to 34 % podniků.

- **Bezpečnostní dokumentaci** definující opatření, postupy a procedury týkající se bezpečnosti ICT v roce 2024 mělo 27 % firem s 10 a více zaměstnanci v ČR. Šlo o 21 % malých subjektů, 46 % středně velkých a více než 82 % velkých podniků. Firmy, které mají vytvořenou bezpečnostní dokumentaci, ji mají nejčastěji (67 % z nich) vytvořenou či naposledy aktualizovanou v posledním roce.
- **S alespoň jedním kybernetickým incidentem** se v průběhu roku 2023 setkalo 27 % podniků s 10 a více zaměstnanci v Česku. Celkový údaj ale značně ovlivňuje velký počet malých firem, u nichž je zkušenost s bezpečnostním incidentem nejméně častá (24 %). S bezpečnostními problémy v oblasti ICT se však potýkala **bezmála polovina velkých podniků** s více než 250 zaměstnanci (48 %) a zkušenost s ním má také 35 % středně velkých firem.
- V evropském srovnání je údaj za Česko 27 % podniků se zkušeností s alespoň jedním kybernetickým incidentem **nadprůměrnou, pátou nejvyšší hodnotou**. Průměr EU27 byl za rok 2023 v tomto ukazateli 22 %. Nejvyšší podíl podniků, které se setkaly s bezpečnostním incidentem, byl v roce 2023 zaznamenán ve Finsku (42 % podniků).
- **Nejčastějším bezpečnostním problémem**, kterému čelily podniky v Česku, byla v roce 2023 **nedostupnost ICT služeb**. Postihla v průměru 23 % podniků s 10 a více zaměstnanci, nejvíce ovšem velké podniky, z nichž to byla téměř polovina (45 %). Nedostupnost služeb – například serveru nebo webových stránek, může způsobit např. technická závada na infrastruktuře nebo i cílený útok zvnějšku, třeba ransomware nebo útok typu odepření služby (Denial of Service, zkratka DoS, nebo DDoS v případě, že jde o distribuovaný útok z mnoha míst). Ransomware je škodlivý vyděračský program, který zapříčiňuje nedostupnost dat nebo celého systému a za znovuobnovení je požadováno zaplacení výkupného.
- Z hlediska příčiny, výsledky šetření ukazují, že nejvíce podniků v Česku čelilo v roce 2023 **nedostupnosti služeb kvůli tzv. vnitřnímu problému** (22 % podniků celkem), tedy např. kvůli selhání hardwaru nebo softwaru. Šlo tedy častěji o technický problém než o útok z vnějšku. **S vnějším útokem, který způsobil nedostupnost služeb ICT, přiznalo zkušenost 5 % podniků** celkem a 8 % velkých podniků s více než 250 zaměstnanci. V evropském srovnání byly české podniky se zkušeností s vnějším útokem způsobujícím nedostupnost služeb ICT nadprůměrné, umístily se za podniky v Lotyšsku, Finsku, Řecku, Maltě a v Nizozemsku na šesté příčce.
- I v případě nedostupnosti služeb ICT je v evropském srovnání údaj za Česko (23 % podniků) **šestou nejvyšší hodnotou**, průměr EU27 byl 19 %. Zůstává i první příčka pro podniky ve Finsku (40 %), na druhém místě jsou podniky v Polsku (30 %) a na třetím na Maltě (25 %).
- **Ztráta firemních dat** patří dlouhodobě mezi méně časté bezpečnostní incidenty. Aby k ní nedocházelo, měly by být veškeré počítače a jejich programové vybavení včetně operačního systému udržovány v aktuálním stavu, počítačové sítě zabezpečeny a firemní data pravidelně zálohována. Ke ztrátě firemních dat může dojít např. napadením škodlivým softwarem (malwarem), tedy nejrůznějšími počítačovými viry, červy, trojskými koni nebo jinými programy, které byly vytvořeny se škodlivým záměrem. Na firemní data mohou rovněž zaútočit hackeři. **Nějaký typ cíleného vnějšího útoku v roce 2023 zaznamenala 2 % firem v Česku.** V evropském srovnání zaujímají české podniky pátou nejvyšší hodnotu, první příčka za rok 2023 patřila podnikům na Maltě, v Rumunsku nebo v Polsku (v každé z těchto zemí se takový útok týkal 3 % podniků).
- Ke **zničení nebo poškození firemních dat** ale může dojít také neúmyslnou chybou zaměstnance nebo vinou technické závady ve firmě, např. chybnou aktualizací nebo selháním hardwaru. Se zničením nebo ztrátou firemních dat kvůli vnitřnímu problému se v roce 2023 setkalo **v České republice 6 % podniků**. Relativně nejvíce tento incident postihl velké podniky (9 %). Z hlediska odvětví pak nejčastěji firmy působící v telekomunikačních činnostech (16 %). V evropském žebříčku jsou v tomto ukazateli tuzemské podniky na čtvrtém místě. Prvenství patří podnikům v Rumunsku (12 %), následované podniky v Polsku (8 %) a na Maltě (7 %).
- V průběhu roku 2023 byl bezpečnostní incident způsobující **prozrazení důvěrných údajů poměrně vzácný** – zkušenost s ním přiznala pouhá 2 % všech firem v Česku, z velkých podniků to bylo 5 %. Řadí se sem např. phishing nebo pharming, kdy se útočník prostřednictvím falešné identity snaží od zaměstnance získat důvěrné informace.

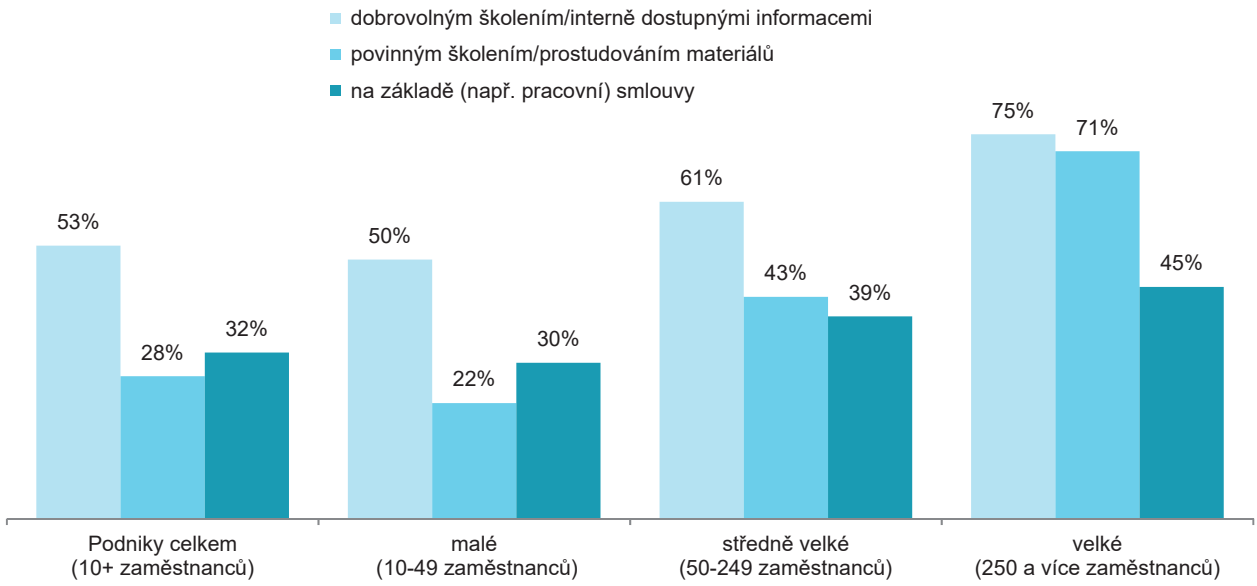
Graf 12.1: Využívání opatření k zajištění kybernetické bezpečnosti podniky v ČR a v zemích EU; 2024



% z celkového počtu podniků s 10 a více zaměstnanci

Zdroj: Český statistický úřad, Eurostat

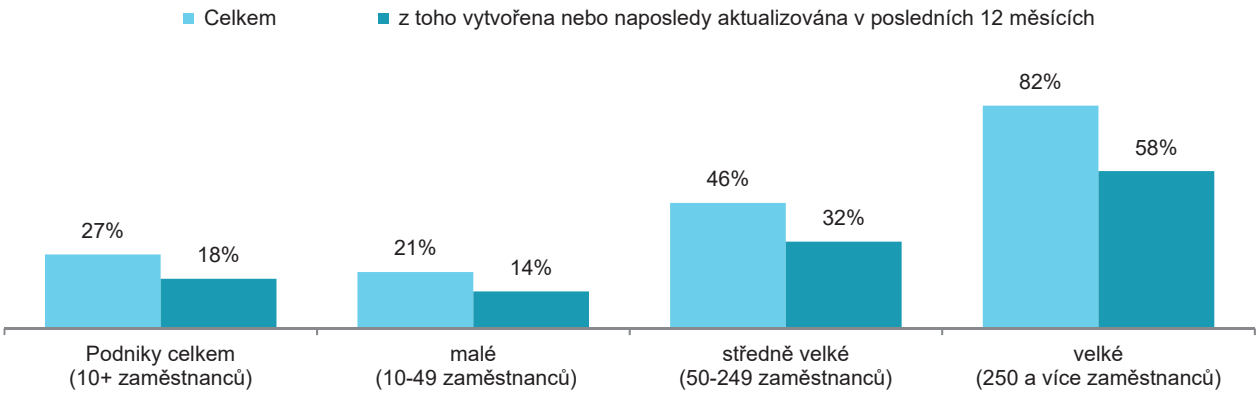
Graf 12.2: Jakými způsoby zajišťovaly podniky v ČR povědomí zaměstnanců o jejich povinnostech souvisejících s kybernetickou bezpečností; 2024



% z celkového počtu podniků s 10 a více zaměstnanci v dané skupině

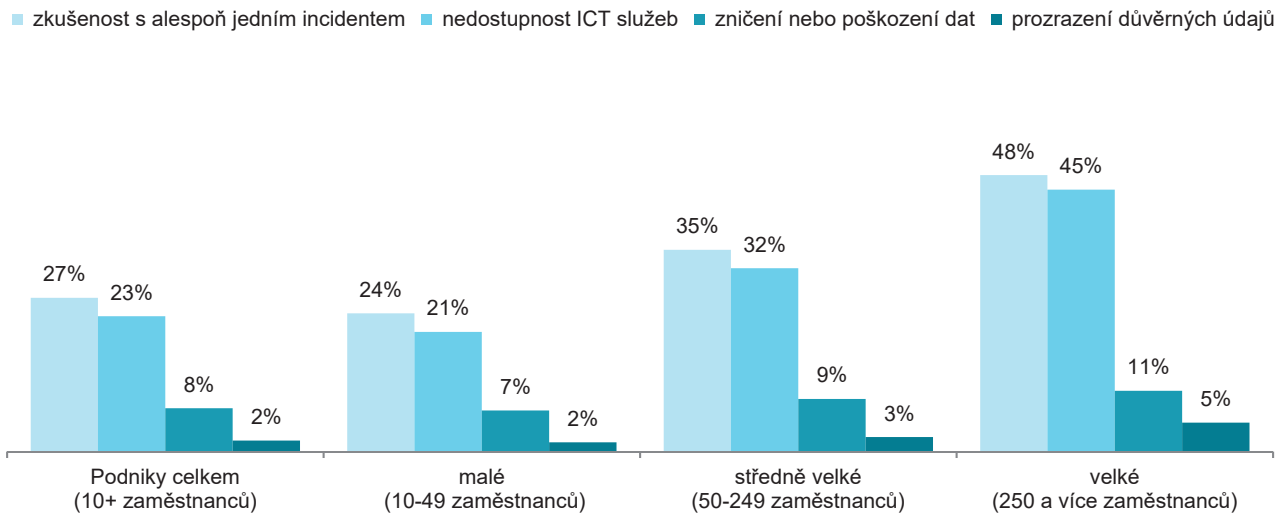
Zdroj: Český statistický úřad

Graf 12.3: Podniky v ČR s vytvořenou bezpečnostní dokumentací; 2024



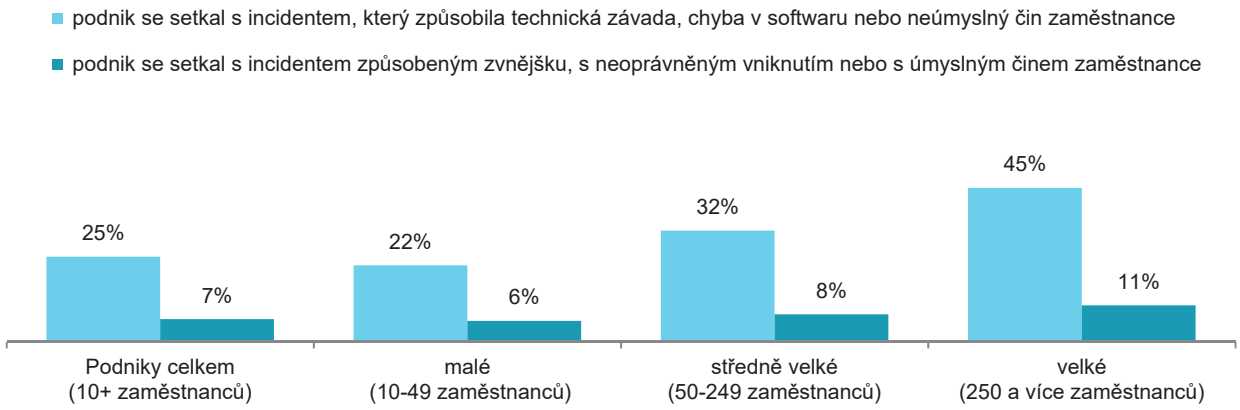
% z celkového počtu podniků s 10 a více zaměstnanci v dané skupině

Graf 12.4: Zkušenosti podniků v ČR s kybernetickými incidenty; 2023



% z celkového počtu podniků s 10 a více zaměstnanci v dané skupině

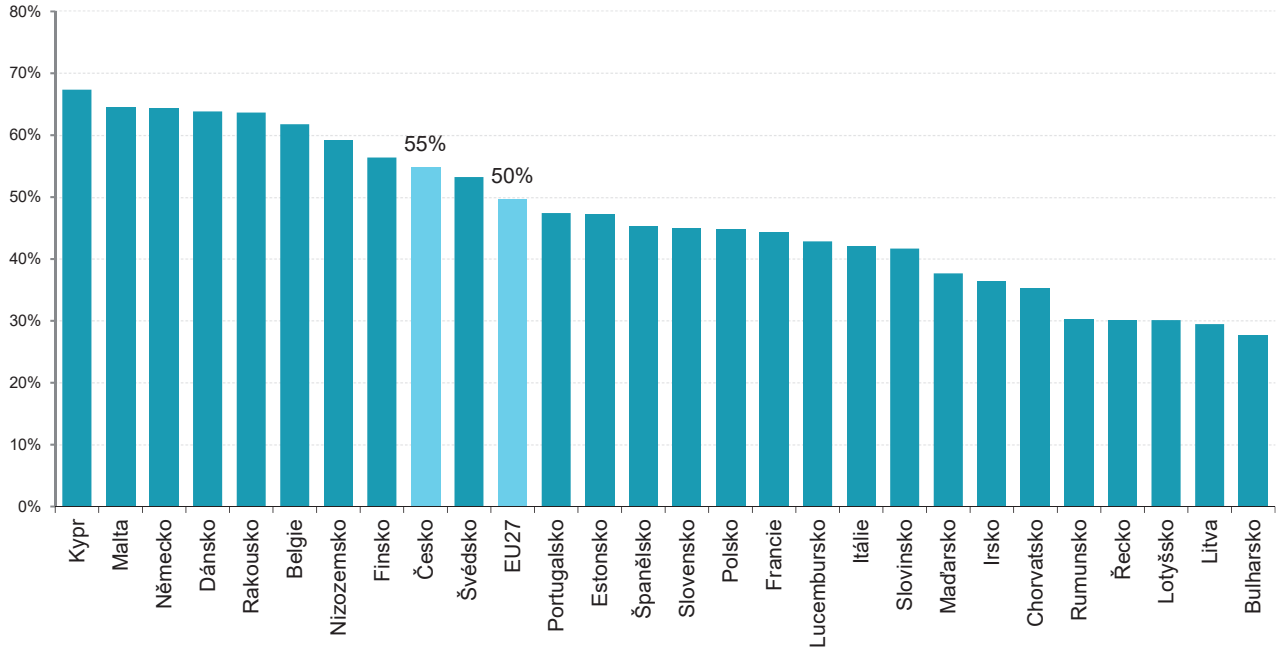
Graf 12.5: Typy kybernetických incidentů v podnicích v ČR; 2023



% z celkového počtu podniků s 10 a více zaměstnanci v dané skupině

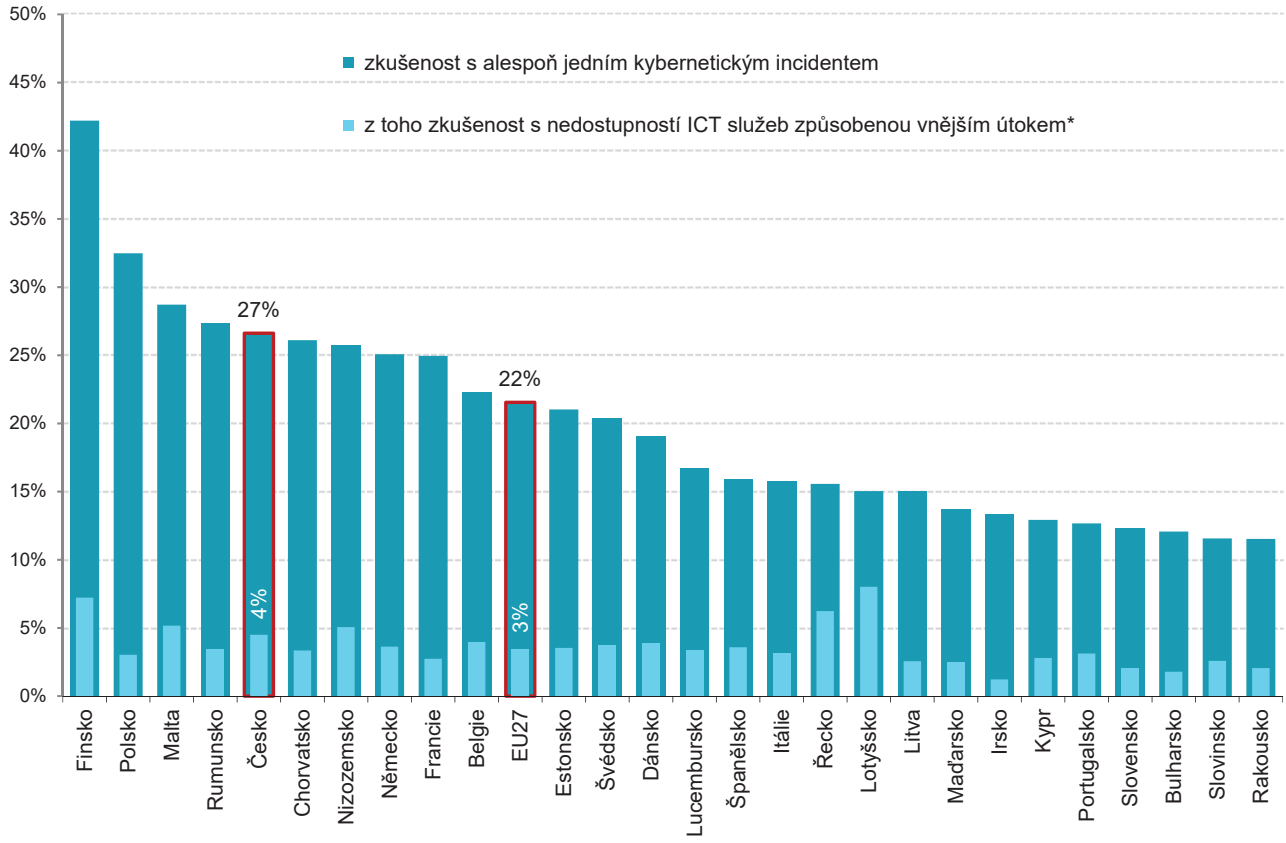
Zdroj: Český statistický úřad

Graf 12.6: Podniky v zemích EU používající VPN sítě; 2024



% z celkového počtu podniků s 10 a více zaměstnanci v dané zemi *zdroj dat: Eurostat, prosinec 2024*

Graf 12.7: Zkušenosti podniků v zemích EU s kybernetickými incidenty; 2023



** např. ransomware (vyděračský software) nebo útok typu odepření služby – Denial of Service (DoS)*

% z celkového počtu podniků s 10 a více zaměstnanci v dané zemi *zdroj dat: Eurostat, prosinec 2024*