# 9. Bezpečnost ICT

*S rozšiřováním informačních a komunikačních technologií vzrůstá i riziko jejich napadení a zneužití získaných informací. Proto je důležité věnovat pozornost jejich zabezpečení. Bezpečnost ICT sleduje zabezpečení celé IT infrastruktury, včetně koncových zařízení. V praxi to znamená ochranu před neoprávněnou fyzickou manipulací se zařízeními, zabezpečení přístupu k elektronickým datům a ochranu před jejich neoprávněnou manipulací, šifrování vzájemné komunikace i uložených dat a jejich pravidelné zálohování.*

## Hlavní zjištění

* Nejběžnějšími opatřeními k zajištění bezpečnosti ICT bylo v roce 2022 používání **silné metody ověření pomocí hesla** do počítače, sítě nebo aplikací a **zálohování** firemních dat na samostatné nebo externí úložiště. Tato dvě opatření využívá 86 respektive 81 % firem v ČR s více než 10 zaměstnanci, velkých firem je dokonce více než 97 %.
* 68 % používá **řízení přístupu** uživatelů a zařízení do podnikové sítě. Kontrolování oprávnění k přístupu k firemním datům se výrazně liší v závislosti na velikosti subjektů. Správu přístupu používá 62 % malých firem, středně velkých subjektů je 88 % a velkých 97 %.
* Více než polovina firem v ČR (56 %) 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 95 % velkých firem, 79 % středně velkých a polovina malých.
* 37 % podniků s 10 a více zaměstnanci **uchovává tzv. logy** (informace sítě a bezpečnostních zařízení) pro následnou analýzu proběhlých bezpečnostních incidentů. Stejný podíl subjektů s 10 a více zaměstnanci v ČR provádí pravidelné **testy bezpečnosti ICT** a podobný podíl firem pravidelně **vyhodnocuje ICT rizika**, resp. pravděpodobnost výskytu bezpečnostních incidentů (35 % firem). Ve všech zmíněných případech platí, že tato opatření praktikují mnohem častěji velké firmy s více než 250 zaměstnanci než malé subjekty.
* Přibližně třetina firem v ČR používala v roce 2022 nástroje pro **šifrování** dat, dokumentů nebo e-mailové komunikace. Šifrovanou komunikaci využívá 27 % malých subjektů, 47 % středně velkých a více než sedm z deseti velkých firem. **Bezpečnostní monitorovací systém**, který dokáže rozpoznat podezřelou aktivitu v ICT systémech a upozornit na ni, používalo v roce 2022 31 % firem s deseti a více zaměstnanci, nevíce opět podniky s více než 250 zaměstnanci (69 % z nich).
* **Rozpoznávání identity uživatelů založené na alespoň dvoufaktorovém způsobu**, tj. například pomocí znalosti hesla a dále díky jednorázovému vygenerovanému heslu či kódu zaslanému prostřednictvím speciální aplikace nebo pomocí SMS je jedna ze dvou nejméně často využívaných opatření k zajištění bezpečnosti ICT v podnicích. Druhou málo frekventovanou metodou je **využívání biometrických metod** k rozpoznávání a ověřování uživatelů. V roce 2022 používalo alespoň dvoufázový způsob rozpoznávání a ověřování identity uživatelů 28 % podniků v Česku a biometrické metody 18 % subjektů, nejčastěji šlo již tradičně o velké subjekty (62 % dvoufázová identifikace, resp. 32 % biometrické metody).
* U všech výše popsaných opatření využívaných firmami k zajištění bezpečnosti ICT platí, že jsou nejvíce uplatňovány subjekty ze sekce CZ NACE J Informační a komunikační činnosti, tedy konkrétně v IT oboru, telekomunikacích a audiovizuálním sektoru.
* **Zajišťování povědomí o povinnostech zaměstnanců souvisejících s bezpečností ICT** se ve firmách v ČR děje nejčastěji dobrovolným školením zaměstnancům, např. zveřejněním informací na intranetu. Tímto způsobem to provádí polovina firem s deseti a více zaměstnanci (52 %), 64 % středně velkých a  80 % velkých subjektů. Dalších 29 % podniků seznamuje své zaměstnance s jejich povinnostmi souvisejícími s bezpečností ICT na povinných kurzech nebo pomocí povinného prostudování materiálů. Povinné školení zaměstnanců praktikují dvě třetiny velkých firem v ČR. Zajištění povědomí o povinnostech souvisejících s bezpečností ICT se dají zakotvit např. do pracovní smlouvy. Tuto možnost využívá 30 % subjektů v ČR, 35 % středně velkých firem a 46 % 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 2022[[1]](#footnote-1) dobrovolné školení zaměstnanců častěji (52 %), než v průměru v ostatních zemích Unie, průměr za EU27 činil 42 %. Povinné školení v oblasti bezpečnosti ICT pořádalo v roce 2022 29 % podniků v ČR, průměr za EU je v tomto případě 21 % podniků a ukotvení povinností souvisejících s bezpečností ICT ve smlouvě, např. v pracovní smlouvě aplikuje 30 % podniků v ČR a v průměru EU je to 32 % podniků.
* **Většina firem v Česku (57 %**) s**i na činnosti související s bezpečností ICT najímá externí pracovníky** či živnostníky, kteří se na ně specializují. Dvě pětiny podniků využívají na činnosti související s bezpečností ICT služby **pouze od zaměstnanců externích subjektů**. Celkový údaj za podniky silně ovlivňuje situace v malých firmách, kde nad všemi dalšími možnostmi převládá **využívání pouze externích IT odborníků (44 %)**. Středně velkých firem, které bezpečnost jejich ICT systémů svěřují pouze externím pracovníkům, je třetina (32 %) a velkých podniků je 7 %.
* I v ostatních zemích EU (s výjimkou Lotyšska) platí, že **na činnosti související s bezpečností ICT si více podniků najímá externí pracovníky** či živnostníky, kteří se na tyto činnosti specializují **než vlastní zaměstnance**. V Lotyšsku platí opačný trend, na činnosti související s bezpečností ICT využívá více tamějších podniků vlastní zaměstnance než externisty. Ve Finsku je situace vyrovnaná. 70 % podniků ve Finsku využívá externisty a 69 % podniků zkušenosti vlastních zaměstnanců.
* Stejně jako u malých subjektů převládá odpověď, že úkony související s bezpečností ICT provádí pouze externí pracovníci, tak u velkých podniků dominuje odpověď, že **tyto činnosti vykonávají různí pracovníci - jak vlastní zaměstnanci, tak i externí pracovníci**. Uvádí to 64 % velkých podniků s více než 250 zaměstnanci. Činnosti související s bezpečností ICT neprovádí 17 % podniků v Česku, nejčastěji jsou to malé firmy (20 %).
* **Bezpečnostní dokumentaci** definující opatření, postupy a procedury týkající se bezpečnosti ICT mělo v roce 2022 26 % firem s 10 a více zaměstnanci v ČR. Šlo 19 % malých subjektů, 43 % středně velkých a více než 81 % velkých subjektů. Firmy, které mají vytvořenou bezpečnostní dokumentaci, ji mají nejčastěji (69 % z nich) vytvořenou či naposledy aktualizovanou v posledním roce.
* S alespoň jedním bezpečnostním incidentem se v průběhu roku 2021 setkalo 29 % firem v ČR. V evropském srovnání jde o nadprůměrnou (čtvrtou nejvyšší) hodnotu, průměr EU 27 je v tomto ukazateli 22 %. **S vnějším kybernetickým útokem se v roce 2021 potýkalo v průměru 7 % podniků** v Česku. Přibližně **čtyřikrát častěji než s vnějšími útoky** se podniky setkaly s bezpečnostními incidenty **způsobenými technickou závadou, chybou v softwaru** nebo v důsledku **neúmyslného činu** vlastního zaměstnance (27 % podniků).
* V roce 2021 nejčastěji podniky postihla **nedostupnost služeb ICT**. Tu může způsobit útok **typu Denial of Service** na počítač nebo síť, který způsobí přehlcení kapacity serveru obrovským množstvím požadavků a tím způsobí jeho nedostupnost. Může jít také o **ransomware**, škodlivý vyděračský program který cílí na nedostupnost dat nebo celého systému a za znovuobnovení je požadováno zaplacení výkupného. S nedostupností ICT služeb se v roce 2021 setkala téměř polovina velkých firem (46 %), 36 % středně velkých a 23 % malých subjektů s 10 až 49 zaměstnanci.
* Mezi méně časté bezpečnostní incidenty patřilo v roce 2021 **zničení nebo poškození firemních dat**. Setkala se s ním 9 % firem v ČR, 14 % velkých podniků. Ke zničení nebo poškození dat firmy může dojít např. kvůli nakažení škodlivým softwarem nebo kvůli neoprávněnému vniknutí (útok hackerů). S tímto typem bezpečnostního útoku se setkaly nejčastěji firmy působící v maloobchodě (16 %), v obchodě či opravách motorových vozidel (12 %) a také v telekomunikačních činnostech (11 %).
* V českém podnikatelském sektoru byl v průběhu roku 2021 útok způsobující **prozrazení důvěrných údajů** poměrně vzácný – zkušenost s ním přiznala pouhá 2 % všech firem s více než 10 zaměstnanci, z velkých subjektů to bylo 6 %. Jde o moderní formy podvodů, které cílí většinou na zaměstnance s cílem získat citlivé informace. Řadí se sem např. **phishing, pharming**, kdy se útočník prostřednictvím falešné identity snaží získat důvěrné informace.
* Proti incidentům v oblasti bezpečnosti ICT může mít firma **sjednané pojištění**, které, v případě, kdy dojde ke kybernetickému útoku, může firmě krýt škody na datech, za nefunkčnost systému nebo třeba odpovědnost za újmu způsobenou únikem dat. Takové pojištění měla ale v roce 2022 sjednáno jen 12 % firem v ČR. Častěji ho měli velké subjekty (29 %) nebo středně velké firmy (16 %) a z hlediska odvětví subjekty působící v činnostech v oblasti IT (42 %).

|  |
| --- |
| **Graf 9.1: Využívání opatření k zajištění bezpečnosti ICT podniky s 10 a více zaměstnanci; 2022***podíl podniků využívajících daná opatření na celkovém počtu podniků s 10 a více zaměstnanci* |
|  |

**Graf 9.2: Provádění činností souvisejících s bezpečností ICT v podnicích s 10 a více zaměstnanci; 2022**

*podíl na celkovém počtu podniků s 10 a více zaměstnanci v dané velikostní skupině*

Zdroj: Český statistický úřad 2022

**Tab. 9.1: Podniky s 10 a více zaměstnanci v ČR využívající opatření k zajištění bezpečnosti ICT; 2022**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | silná metoda ověření pomocí hesla | zálohování dat na samostatné/ externí úložiště | správa přístupu uživatelských práv do firemní sítě | používání VPN sítí | uchovávání logů pro následnou analýzu proběhlých incidentů |
|  |
| **Podniky celkem (10+)** | **86,5**  | **81,2**  | **67,7**  | **55,6**  | **37,0**  |
| **Velikost podniku** |  |  |  |  |  |
|  10–49 zaměstnanců | 84,0  | 78,2  | 61,8  | 48,6  | 29,7  |
|  50–249 zaměstnanců | 95,4  | 91,4  | 88,3  | 78,9  | 60,7  |
|  250 a více zaměstnanců | 97,8  | 97,1  | 97,2  | 95,0  | 79,9  |
| **Odvětví (ekonomická činnost)** |  |  |  |  |  |
|  Zpracovatelský průmysl | 90,2  | 86,2  | 73,6  | 59,9  | 37,1  |
|  Výroba a rozvod energie, plynu, tepla | 90,8  | 88,0  | 69,9  | 57,9  | 42,1  |
|  Stavebnictví | 80,0  | 73,5  | 56,0  | 38,2  | 19,0  |
|  Obchod a opravy motorových vozidel | 93,4  | 90,6  | 78,0  | 67,9  | 43,9  |
|  Velkoobchod | 89,9  | 88,3  | 76,8  | 69,2  | 45,5  |
|  Maloobchod | 84,1  | 78,1  | 63,8  | 42,7  | 32,9  |
|  Doprava a skladování | 83,4  | 73,9  | 54,9  | 45,4  | 26,5  |
|  Ubytování | 92,2  | 82,0  | 72,1  | 54,9  | 39,9  |
|  Stravování a pohostinství | 69,9  | 49,6  | 32,7  | 24,0  | 11,9  |
|  Činnosti cestovních agentur a kanceláří | 92,7  | 91,4  | 82,1  | 71,9  | 49,9  |
|  Audiovizuální činnosti; vydavatelství | 93,2  | 95,6  | 89,0  | 82,2  | 69,6  |
|  Telekomunikační činnosti | 95,8  | 93,8  | 91,6  | 91,2  | 82,3  |
|  Činnosti v oblasti IT | 96,7  | 96,1  | 94,1  | 92,7  | 81,4  |
|  Činnosti v oblasti nemovitostí | 85,2  | 85,7  | 72,7  | 57,6  | 41,5  |
|  Profesní, vědecké a technické činnosti | 90,4  | 92,7  | 84,9  | 76,4  | 59,5  |
|  Ostatní administrativní a podpůrné činnosti | 80,5  | 68,1  | 51,6  | 41,8  | 29,8  |

*podíl na celkovém počtu podniků s 10 a více zaměstnanci v dané velikostní a odvětvové skupině (v %)*

**Tab. 9.2: Podniky s 10 a více zaměstnanci v ČR využívající opatření k zajištění bezpečnosti ICT; 2022 – pokračování**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | pravidelné testy bezpečno-sti ICT | pravidel-né vyhodno-cování ICT rizik | nástroje pro šifrování dat, dokumentů nebo e-mailů | bezpečno-stní monitorova-cí systém | ověřování identity uživatelů pomocí alespoň dvoufázového způsobu  | ověřování identity uživatelů pomocí biometric-kých metod |
|  |
| **Podniky celkem (10+)** | **36,8**  | **35,4**  | **32,1**  | **30,7**  | **27,6**  | **18,0**  |
| **Velikost podniku** |  |  |  |  |  |  |
|  10–49 zaměstnanců | 31,7  | 29,0  | 27,0  | 25,5  | 24,4  | 16,6  |
|  50–249 zaměstnanců | 52,8  | 56,3  | 46,7  | 45,7  | 34,5  | 21,5  |
|  250 a více zaměstnanců | 69,3  | 74,7  | 71,0  | 69,4  | 61,8  | 32,4  |
| **Odvětví (ekonomická činnost)** |  |  |  |  |  |  |
|  Zpracovatelský průmysl | 38,3  | 37,6  | 30,8  | 31,7  | 25,7  | 16,2  |
|  Výroba a rozvod energie, plynu, tepla | 35,4  | 34,1  | 36,3  | 33,1  | 24,2  | 15,3  |
|  Stavebnictví | 27,7  | 22,0  | 18,9  | 16,7  | 18,0  | 16,9  |
|  Obchod a opravy motorových vozidel | 36,2  | 35,7  | 35,3  | 30,9  | 38,3  | 25,2  |
|  Velkoobchod | 41,8  | 41,4  | 35,9  | 38,6  | 28,8  | 20,3  |
|  Maloobchod | 32,8  | 31,2  | 27,3  | 22,8  | 21,6  | 10,1  |
|  Doprava a skladování | 30,4  | 26,6  | 21,0  | 26,8  | 28,6  | 17,5  |
|  Ubytování | 34,5  | 36,1  | 32,7  | 29,0  | 30,3  | 11,9  |
|  Stravování a pohostinství | 13,5  | 12,4  | 12,3  | 13,0  | 14,2  | 12,6  |
|  Činnosti cestovních agentur a kanceláří | 45,5  | 45,5  | 34,1  | 30,2  | 38,0  | 14,0  |
|  Audiovizuální činnosti; vydavatelství | 51,4  | 57,9  | 54,0  | 44,5  | 47,8  | 26,1  |
|  Telekomunikační činnosti | 56,9  | 63,6  | 65,4  | 56,9  | 46,9  | 28,5  |
|  Činnosti v oblasti IT | 70,0  | 74,1  | 79,1  | 64,4  | 68,5  | 40,5  |
|  Činnosti v oblasti nemovitostí | 38,0  | 37,3  | 33,6  | 29,0  | 26,4  | 18,4  |
|  Profesní, vědecké a technické činnosti | 56,2  | 54,7  | 55,8  | 49,3  | 40,2  | 23,4  |
|  Ostatní administrativní a podpůrné činnosti | 28,5 | 28,1 | 30,5 | 24,3 | 25,2 | 17,8 |

*podíl na celkovém počtu podniků s 10 a více zaměstnanci v dané velikostní a odvětvové skupině (v %)*

Zdroj: Český statistický úřad 2022

**Tab. 9.3: Bezpečnostní dokumentace a zkušenost s bezpečnostními incidenty v podnicích s 10 a více zaměstnanci v ČR; 2022**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|   | podniky s vytvořenou ICT bezpečnostní dokumentací | z toho: tato dokumentace byla vytvořena/ aktualizována v posled.roce | podniky se zkušeností s alespoň jedním bezpečnostním incidentem v roce 2021 | podniky, které se v roce 2021 potýkaly s nedostupností služeb ICT | podniky, které mají pojištění proti incidentům v oblasti bezpečnosti ICT |
|
| **Podniky celkem (10+)** | **25,8**  | **17,7**  | **29,3**  | **26,4**  | **11,6**  |
| **Velikost podniku** |   |   |  |   |  |
|  10–49 zaměstnanců | 19,4  | 12,9  | 26,1  | 23,4  | 9,9  |
|  50–249 zaměstnanců | 42,8  | 30,0  | 39,6  | 36,2  | 15,7  |
|  250 a více zaměstnanců | 81,4  | 60,0  | 50,2  | 45,7  | 29,1  |
| **Odvětví (ekonomická činnost)** |   |   |  |   |  |
|  Zpracovatelský průmysl | 26,5  | 16,4  | 30,4  | 27,5  | 11,8  |
|  Výroba a rozvod energie, plynu, tepla | 32,6  | 18,4  | 28,6  | 28,0  | 9,1  |
|  Stavebnictví | 11,1  | 7,6  | 21,1  | 18,9  | 5,9  |
|  Obchod a opravy motorových vozidel | 30,2  | 18,2  | 45,5  | 42,1  | 13,9  |
|  Velkoobchod | 31,7  | 25,3  | 31,6  | 27,5  | 13,1  |
|  Maloobchod | 21,7  | 14,3  | 36,3  | 33,5  | 7,4  |
|  Doprava a skladování | 16,4  | 12,9  | 18,2  | 14,8  | 5,1  |
|  Ubytování | 22,4  | 12,8  | 27,5  | 26,2  | 11,0  |
|  Stravování a pohostinství | 6,7  | 3,6  | 21,3  | 19,2  | 6,5  |
|  Činnosti cestovních agentur a kanceláří | 35,8  | 27,7  | 30,4  | 26,3  | 10,3  |
|  Audiovizuální činnosti; vydavatelství | 49,5  | 32,4  | 44,1  | 42,5  | 22,4  |
|  Telekomunikační činnosti | 60,7  | 41,3  | 48,4  | 45,5  | 23,1  |
|  Činnosti v oblasti IT | 69,4  | 55,9  | 44,0  | 42,3  | 42,0  |
|  Činnosti v oblasti nemovitostí | 28,2  | 16,9  | 29,6  | 24,8  | 13,9  |
|  Profesní, vědecké a technické činnosti | 41,7  | 29,2  | 36,9  | 33,1  | 20,4  |
|  Ostatní administrativní a podpůrné činnosti | 22,4  | 14,6  | 22,9  | 20,9  | 6,1  |

*podíl na celkovém počtu podniků s 10 a více zaměstnanci v dané velikostní a odvětvové skupině (v %)*

**Graf 9.3: Jakými způsoby zajišťovaly podniky s 10 a více zaměstnanci v ČR u zaměstnanců povědomí o jejich povinnostech souvisejících s bezpečností ICT; 2022**

*podíl na celkovém počtu podniků s 10 a více zaměstnanci v dané odvětvové skupině*

Zdroj: Český statistický úřad 2022

**Graf 9.4: Kdo v podnicích v zemích EU provádí činnosti související s bezpečností ICT; 2022**

(respondenti měli možnost uvést obě nabízené odpovědi)

****

*\* jde o vlastní zaměstnance podniku nebo zaměstnance mateřské firmy či jiných příbuzných firem v rámci skupiny podniků*

*podíl na celkovém počtu podniků s 10 a více zaměstnanci v dané zemi zdroj dat: Eurostat, prosinec 2022*

**Graf 9.5: Zkušenosti podniků v zemích EU s bezpečnostními incidenty; 2021**

****

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

*podíl na celkovém počtu podniků s 10 a více zaměstnanci v dané zemi zdroj dat: Eurostat, prosinec 2022*

1. Zdrojem dat pro mezinárodní srovnání je databáze Eurostatu, která byla aktualizována na začátku prosince 2022 a údaje v ní se vztahují k roku 2022, někde k roku 2021: [http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database](http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database%20%20)  [↑](#footnote-ref-1)