# 8. Zkušenosti podniků s bezpečnostními incidenty souvisejícími s ICT

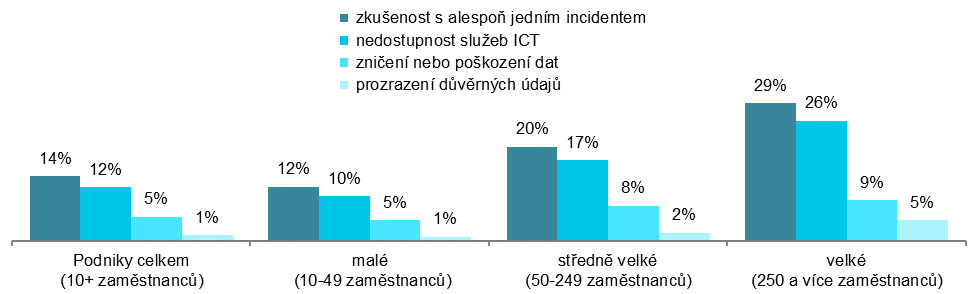
*S rozšiřováním informačních a komunikačních technologií vzrůstá i riziko jejich napadení a poškození či zneužití získaných informací. Proto je důležité věnovat pozornost bezpečnosti ICT, která sleduje zabezpečení celé IT infrastruktury včetně koncových zařízení. V praxi to znamená ochranu před neoprávněnou 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.*

*Pozn.: otázky v této kapitole se vztahují k roku předcházejícímu šetření, tj. zde konkrétně k roku 2020*

## Hlavní zjištění

* **S alespoň jedním ICT bezpečnostním incidentem** se v průběhu roku 2020 setkalo 14 % podniků s deseti a více zaměstnanci v ČR. Mezi velkými podniky se tak stalo u 29 % z nich, ale tyto bezpečnostní incidenty se nevyhnuly ani pětině středně velkých subjektů a 12 % malých firem. S některým z bezpečnostních incidentů souvisejících s ICT se setkaly nejčastěji podniky působící v oboru telekomunikační činnosti (38 % z nich), ale také 27 % firem působících v oblasti IT nebo 22 % subjektů z oboru obchod a opravy motorových vozidel.
* Nejčastějším bezpečnostním incidentem byla v roce 2020 **nedostupnost služeb ICT**. S nedostupností ICT služeb se v roce 2020 v Česku setkalo celkem 12 % podniků. Zkušenost s ní má 26 % velkých podniků, 17 % středně velkých a desetina malých subjektů s 10 až 49 zaměstnanci. Může jít o útok typu odepření služby(Denial of Service; DoS, příp. DDoS), což je typ útoku na počítač nebo síť, který způsobí přehlcení kapacity serveru obrovským množstvím požadavků a tím způsobí jeho nedostupnost. Dalším útokem může být také napadení vyděračským programem (ransomwarem), který cílí na nedostupnost dat nebo celého systému a za znovuobnovení je požadováno zaplacení výkupného.
* Mezi méně časté bezpečnostní incidenty patřilo v roce 2020 **zničení nebo poškození firemních dat**. Setkalo se s ním 5 % podniků s deseti a více zaměstnanci, ale téměř desetina velkých subjektů (9 %). Ke zničení nebo poškození dat firmy může dojít např. kvůli nakažení škodlivým softwarem nebo neoprávněnému vniknutí (útok hackerů). I s tímto typem bezpečnostního útoku se setkaly nejčastěji firmy působící v telekomunikačních činnostech (11 %) nebo v činnostech v oblasti IT (9 %).
* Poměrně vzácný byl v českém podnikatelském sektoru v průběhu roku 2020 útok způsobující **prozrazení důvěrných údajů** – zkušenost s ním deklarovalo jen 1 % všech firem s více než 10 zaměstnanci, z velkých subjektů to bylo 5 %. Jde o moderní formy podvodů, které cílí většinou na zaměstnance s cílem získat citlivé informace. Řadí se sem např. phishing a pharming, kdy se útočník prostřednictvím falešné identity snaží získat důvěrné informace. S tímto typem útoku mají zkušenost nejvíce podniky z telekomunikačních činností (4 %) případně cestovní agentury a kanceláře (3 %).
* Pro **evropské srovnání** zkušeností podniků s bezpečnostními incidenty souvisejícími s ICT jsou v době vydání publikace k dispozici jen data za rok 2019. Tehdy se s alespoň jedním bezpečnostním incidentem souvisejícím s ICT setkala pětina podniků s 10 a více zaměstnanci v Česku, což byl čtvrtý nejčastější podíl v rámci Unie. První tři příčky obsadily podniky ve Švédsku (35 %), na Maltě (24 %) a v Belgii (22 %), průměr za EU byl v tomto ukazateli 13 %.

**Graf 8.1: Zkušenost s bezpečnostními incidenty ICT v roce 2020 v podnicích s 10 a více zaměstnanci v ČR**

**

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

Zdroj: Český statistický úřad 2021

**Tab. 8.1: Zkušenost s bezpečnostními incidenty ICT v roce 2020 v podnicích s 10 a více zaměstnanci v ČR**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Podniky, které se setkaly s některým  z bezpečnostních incidentů  souvisejících s ICT | ICT bezpečnostní incident souvisel: | | |
| s nedostupností služeb ICT | se zničením nebo poškozením dat | s prozrazením důvěrných údajů |
| **Podniky celkem (10+)** | **13,8** | **11,5** | **5,2** | **1,3** |
| **Velikost podniku** |  |  |  |  |
| 10–49 zaměstnanců | 11,6 | 9,6 | 4,5 | 1,0 |
| 50–249 zaměstnanců | 20,1 | 17,2 | 7,6 | 1,8 |
| 250 a více zaměstnanců | 29,4 | 25,7 | 8,7 | 4,5 |
| **Odvětví (ekonomická činnost)** |  |  |  |  |
| Zpracovatelský průmysl | 12,7 | 10,5 | 4,7 | 1,6 |
| Výroba a rozvod energie, plynu, tepla | 13,1 | 11,3 | 4,8 | 0,9 |
| Stavebnictví | 10,9 | 7,8 | 4,4 | 0,9 |
| Obchod a opravy motorových vozidel | 22,4 | 19,9 | 7,6 | 1,0 |
| Velkoobchod | 15,5 | 14,7 | 4,8 | 0,7 |
| Maloobchod | 17,3 | 13,8 | 5,8 | 1,3 |
| Doprava a skladování | 10,2 | 8,8 | 4,9 | 1,1 |
| Ubytování | 9,6 | 6,3 | 5,2 | . |
| Stravování a pohostinství | 6,5 | 4,3 | 4,5 | 0,4 |
| Činnosti cestovních agentur a kanceláří | 20,1 | 18,3 | 6,0 | 3,4 |
| Audiovizuální činnosti; vydavatelství | 21,5 | 18,0 | 7,2 | 2,6 |
| Telekomunikační činnosti | 38,2 | 36,2 | 10,9 | 4,0 |
| Činnosti v oblasti IT | 26,5 | 23,3 | 9,2 | 2,6 |
| Činnosti v oblasti nemovitostí | 14,8 | 14,2 | 6,9 | 1,5 |
| Profesní, vědecké a technické činnosti | 18,4 | 15,7 | 5,6 | 1,4 |
| Ostatní administrativní a podpůrné činnosti | 10,7 | 8,0 | 4,6 | 2,0 |

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

Zdroj: Český statistický úřad 2021

**Graf 8.2 Podniky s 10 a více zaměstnanci v zemích EU a jejich zkušenost s bezpečnostními incidenty ICT v roce 2019**



*podíl na celkovém počtu podniků s 10 a více zaměstnanci v dané zemi zdroj dat: Eurostat, prosinec 2019*