# 6. 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 byly na začátku roku 2019 **pravidelná aktualizace** softwarového vybavení používaného ve firmě, používání **silného hesla** do počítače, sítě nebo aplikací a **zálohování** firemních dat na samostatné nebo externí úložiště. Tato tři opatření využívá více než 80 % firem v ČR s více než 10 zaměstnanci, velkých firem je dokonce více než 95 %.
* Více než 60 % firem používá **řízení přístupu** uživatelů a zařízení do podnikové sítě. Kontrolování oprávnění k přístupu do objektu nebo k firemním datům se výrazně liší v závislosti na velikosti subjektů. Správu přístupu používá 54 % malých firem, středně velkých subjektů je 85 % a velkých 96 %.
* Téměř polovina firem v ČR (49 %) používá **virtuální privátní síť (VPN)**, která zprostředkovává zabezpečený vzdálený přístup z jakéhokoli místa prostřednictvím internetu do firemní počítačové sítě. I v tomto případě platí, že používání VPN se významně liší podle velikosti firem. Vzdálený přístup pomocí VPN používá 93 % velkých subjektů, tři čtvrtiny středně velkých firem a dvě pětiny malých firem.
* Přibližně dvě pětiny subjektů s 10 a více zaměstnanci v ČR provádějí pravidelné **testy bezpečnosti ICT** (39 %) a podobný podíl firem pravidelně **vyhodnocuje ICT rizika**, resp. pravděpodobnost výskytu bezpečnostních incidentů (37 % firem). Dvě pětiny subjektů s 10 a více zaměstnanci **uchovávají tzv. logy** (informace sítě a bezpečnostních zařízení) pro následnou analýzu proběhlých bezpečnostních incidentů. Ve všech zmíněných případech platí, že tato opatření praktikují mnohem častěji velké firmy s více než 250 zaměstnanci než malé subjekty.
* Více než třetina firem v ČR používala v roce 2019 nástroje pro **šifrování** dat, dokumentů nebo e-mailové komunikace. Šifrovanou komunikaci využívá 30 % malých subjektů, více než 51 % středně velkých a více než 71 % velkých firem.
* Rozpoznávání a ověřování uživatelů pomocí **biometrických metod** není zatím v českém podnikatelském prostředí příliš rozšířené - v roce 2019 toto opatření používalo 11 % firem celkem, nejčastěji šlo již tradičně o velké subjekty (28 %).
* U všech výše popsaných opatření platí, že jejich používání je typické pro subjekty ze sekce CZ NACE J nazvané Informační a komunikační činnosti, tedy konkrétně v IT odvětví, 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, dvě třetiny středně velkých a 77 % velkých subjektů. Dalších 31 % 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 třetina subjektů v ČR, téměř polovina středně velkých firem a 52 % velkých firem.
* **Úkony související s bezpečností ICT** vykonávali v roce 2019častěji externisté (66 %) než vlastní zaměstnanci firem (37 %). V případě velkých subjektů s více než 250 zaměstnanci je poměr obrácený: ve velkých firmách provádějí činnosti související s bezpečností ICT častěji vlastní zaměstnanci firmy (79 %) než externisté (60 %), i když ani jejich podíl není rozhodně zanedbatelný.
* **Bezpečnostní dokumentaci** definující opatření, postupy a procedury týkající se bezpečnosti ICT měla v roce 2019 třetina firem s 10 a více zaměstnanci v ČR. Šlo o čtvrtinu malých subjektů, více než polovinu středně velkých a 74 % velkých subjektů. Osm firem z deseti má bezpečnostní dokumentaci vytvořenou nebo naposledy aktualizovanou v posledních 12 měsících.

## Bezpečnostní incidenty

* S alespoň jedním bezpečnostním incidentem se v průběhu roku 2018 setkalo více než 20 % firem v ČR. Nejčastěji se jednalo o **nedostupnost služeb ICT**. Může jít o útok **typu Denial of Service**, 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 **ransomware**, který cílí na nedostupnost dat nebo celého systému a za znovuobnovení je požadováno zaplacení výkupného. S nedostupností ICT služeb se v roce 2018 setkala téměř třetina velkých firem, čtvrtina středně velkých a 14 % malých subjektů s 10 až 49 zaměstnanci.
* Mezi méně časté bezpečnostní incidenty patřilo v roce 2018 **zničení nebo poškození firemních dat**. Setkala se s ním desetina firem v ČR, téměř pětina velkých subjektů (17 %). Ke zničení nebo poškození dat firmy může dojít např. kvůli nakažení škodlivým softwarem nebo neoprávněnému vniknutí (útok hackerů). S tímto typem bezpečnostního útoku se setkaly nejčastěji firmy působící s audiovizuálním sektoru (19 %), v elektrotechnickém či strojírenském průmyslu nebo v činnostech v oblasti IT (14 %).
* V českém podnikatelském sektoru byl v průběhu roku 2018 útok způsobující **prozrazení důvěrných údajů** poměrně vzácný – zkušenost s ním přiznalo pouhé 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, pharming**, kdy se útočník prostřednictvím falešné identity snaží získat důvěrné informace.
* Proti incidentům v oblasti bezpečnosti ICT může mít firma **sjednané pojištění**. V případě, kdy dojde ke kybernetickému útoku, pojištění může firmě krýt škody na datech, nefunkčnost systému nebo třeba odpovědnost za újmu způsobenou únikem dat. Takové pojištění měla ale v roce 2019 sjednaná jen necelá desetina firem v ČR. Častěji měli pojištění kybernetických rizik velké subjekty (17 %) nebo středně velké firmy s 50 až 250 zaměstnanci (14 %). Podle odvětví měl o pojištění proti bezpečnostním incidentům relativně největší zájem sektor Informační a komunikační činnosti, zejména pak činnosti v oblasti IT (32 %), případně telekomunikační firmy (19 %).

|  |
| --- |
| **Graf 6.1: Využívání opatření k zajištění bezpečnosti ICT firmami s 10 a více zaměstnanci v ČR v r. 2019***podíl firem využívajících daná opatření na celkovém počtu firem s 10 a více zaměstnanci* |

Zdroj: Český statistický úřad 2019

**Tab. 6.1: Firmy s 10 a více zaměstnanci v ČR využívající opatření k zajištění bezpečnosti ICT v r. 2019**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|   | silné heslo do počítače, sítě nebo aplikací | pravidelná aktualizace SW vybavení | rozpoznání a ověření uživatelů pomocí biometrických metod | nástroje pro šifrování dat, dokumentů nebo e-mailů | zálohování firemních dat na samostatné či externí úložiště |
|
| **Firmy celkem (10+)** | **85,7**  | **88,6**  | **11,2**  | **35,8**  | **81,8**  |
| **Velikost firmy** |   |   |   |   |  |
|  10–49 zaměstnanců | 83,4  | 86,4  | 8,5  | 30,4  | 78,2  |
|  50–249 zaměstnanců | 93,7  | 96,3  | 19,2  | 51,6  | 94,8  |
|  250 a více zaměstnanců | 96,4  | 98,3  | 27,8  | 71,6  | 95,9  |
| **Odvětví (ekonomická činnost)** |   |   |   |   |  |
|  Zpracovatelský průmysl | 87,2  | 90,4  | 10,8  | 33,9  | 85,5  |
|  Výroba a rozvod energie, plynu, tepla | 88,5  | 93,1  | 13,4  | 42,0  | 88,1  |
|  Stavebnictví | 80,1  | 81,9  | 8,4  | 22,6  | 73,2  |
|  Obchod a opravy motorových vozidel | 91,3  | 92,8  | 10,1  | 35,9  | 88,1  |
|  Velkoobchod | 88,9  | 91,8  | 12,0  | 39,8  | 90,9  |
|  Maloobchod | 81,5  | 84,6  | 10,2  | 43,3  | 74,9  |
|  Doprava a skladování | 82,9  | 88,1  | 11,3  | 28,7  | 78,0  |
|  Ubytování | 91,2  | 93,5  | 5,2  | 31,2  | 78,4  |
|  Stravování a pohostinství | 74,5  | 73,5  | 5,0  | 17,0  | 57,2  |
|  Činnosti cestovních agentur a kanceláří | 92,3  | 92,9  | 11,7  | 39,0  | 85,8  |
|  Audiovizuální činnosti; vydavatelství | 94,0  | 96,5  | 20,2  | 63,6  | 92,6  |
|  Telekomunikační činnosti | 96,6  | 97,2  | 23,9  | 64,5  | 91,0  |
|  Činnosti v oblasti IT | 97,3  | 97,1  | 37,1  | 78,7  | 95,1  |
|  Činnosti v oblasti nemovitostí | 85,0  | 90,8  | 12,0  | 40,2  | 84,1  |
|  Profesní, vědecké a technické činnosti | 90,3  | 94,5  | 12,3  | 47,2  | 91,4  |
|  Ostatní administrativní a podpůrné činnosti | 83,2  | 87,5  | 8,7  | 39,6  | 73,7  |

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

**Tab. 6.2: Firmy s 10 a více zaměstnanci v ČR využívající opatření k zajištění bezpečnosti ICT v r. 2019 – pokračování**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|   | správa přístupu uživatelů a zařízení do podnikové sítě | používání VPN sítí | uchovávání logů pro následnou analýzu bezpeč.incidentů | pravidelné vyhodnocování ICT rizik | provádění pravidelných testů bezpečnosti ICT |
|
| **Firmy celkem (10+)** | **61,4**  | **49,1**  | **40,3**  | **36,6**  | **38,6**  |
| **Velikost firmy** |   |   |   |   |  |
|  10–49 zaměstnanců | 54,3  | 40,9  | 32,3  | 30,5  | 35,1  |
|  50–249 zaměstnanců | 85,4  | 75,6  | 66,2  | 55,0  | 48,7  |
|  250 a více zaměstnanců | 96,0  | 93,2  | 81,5  | 73,3  | 63,4  |
| **Odvětví (ekonomická činnost)** |   |   |   |   |  |
|  Zpracovatelský průmysl | 66,5  | 50,7  | 40,9  | 35,7  | 38,1  |
|  Výroba a rozvod energie, plynu, tepla | 73,8  | 64,0  | 57,7  | 52,0  | 47,2  |
|  Stavebnictví | 41,8  | 29,5  | 21,9  | 22,5  | 29,7  |
|  Obchod a opravy motorových vozidel | 74,1  | 53,7  | 44,0  | 42,3  | 45,2  |
|  Velkoobchod | 75,5  | 67,0  | 54,7  | 45,8  | 43,2  |
|  Maloobchod | 53,7  | 46,1  | 37,5  | 33,8  | 38,5  |
|  Doprava a skladování | 50,8  | 41,2  | 27,8  | 27,8  | 35,8  |
|  Ubytování | 62,1  | 41,7  | 37,2  | 36,1  | 39,7  |
|  Stravování a pohostinství | 29,1  | 21,2  | 14,3  | 14,3  | 21,7  |
|  Činnosti cestovních agentur a kanceláří | 79,8  | 63,1  | 51,4  | 48,1  | 53,4  |
|  Audiovizuální činnosti; vydavatelství | 85,3  | 77,7  | 67,4  | 62,9  | 57,4  |
|  Telekomunikační činnosti | 87,4  | 84,8  | 83,3  | 73,5  | 63,7  |
|  Činnosti v oblasti IT | 90,7  | 87,9  | 81,8  | 73,2  | 64,8  |
|  Činnosti v oblasti nemovitostí | 67,2  | 49,5  | 46,7  | 40,9  | 36,2  |
|  Profesní, vědecké a technické činnosti | 76,3  | 63,2  | 56,5  | 52,1  | 50,5  |
|  Ostatní administrativní a podpůrné činnosti | 48,2  | 36,8  | 31,8  | 32,3  | 31,0  |

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

Zdroj: Český statistický úřad 2019

**Tab. 6.3: Bezpečnostní dokumentace v roce 2019 a zkušenost s bezpečnostními incidenty v roce 2018 ve firmách s 10 a více zaměstnanci v ČR**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|   | Firmy s vytvořenou bezpečnostní dokumentací | z toho: tato dokumentace byla vytvořena/ aktualizována v posled.roce | Firmy se zkušeností s alespoň jedním bezpečnostním incidentem | Firmy, které se potýkaly s nedostupností služeb ICT | Firmy, které mají pojištění proti incidentům v oblasti bezpečnosti ICT |
|
| **Firmy celkem (10+)** | **32,1**  | **25,7**  | **20,9**  | **16,5**  | **8,3**  |
| **Velikost firmy** |   |   |   |   |   |
|  10–49 zaměstnanců | 25,6  | 21,2  | 17,7  | 13,6  | 6,7  |
|  50–249 zaměstnanců | 51,5  | 37,8  | 31,2  | 25,8  | 13,7  |
|  250 a více zaměstnanců | 73,8  | 59,3  | 39,0  | 31,9  | 17,0  |
| **Odvětví (ekonomická činnost)** |   |   |   |   |   |
|  Zpracovatelský průmysl | 32,0  | 25,2  | 20,6  | 15,5  | 7,3  |
|  Výroba a rozvod energie, plynu, tepla | 42,2  | 38,3  | 24,8  | 21,6  | 9,3  |
|  Stavebnictví | 17,6  | 12,7  | 15,0  | 11,0  | 5,4  |
|  Obchod a opravy motorových vozidel | 37,3  | 30,8  | 27,6  | 21,3  | 6,3  |
|  Velkoobchod | 38,8  | 26,5  | 27,3  | 24,0  | 6,8  |
|  Maloobchod | 25,8  | 22,5  | 18,9  | 14,1  | 6,5  |
|  Doprava a skladování | 24,7  | 20,8  | 16,1  | 10,8  | 8,3  |
|  Ubytování | 31,1  | 25,0  | 20,2  | 16,0  | 10,4  |
|  Stravování a pohostinství | 14,8  | 11,3  | 13,1  | 10,1  | 4,6  |
|  Činnosti cestovních agentur a kanceláří | 43,9  | 36,1  | 21,6  | 18,5  | 11,2  |
|  Audiovizuální činnosti; vydavatelství | 49,4  | 40,6  | 38,3  | 33,3  | 13,5  |
|  Telekomunikační činnosti | 58,8  | 48,1  | 43,9  | 41,9  | 19,1  |
|  Činnosti v oblasti IT | 65,2  | 59,5  | 38,7  | 36,1  | 31,6  |
|  Činnosti v oblasti nemovitostí | 35,8  | 25,6  | 21,5  | 15,6  | 11,5  |
|  Profesní, vědecké a technické činnosti | 47,9  | 40,3  | 23,0  | 17,4  | 12,2  |
|  Ostatní administrativní a podpůrné činnosti | 33,2  | 29,4  | 18,4  | 16,4  | 8,8  |

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

**Graf 6.2: Jakými způsoby zajišťují firmy s 10 a více zaměstnanci v ČR v roce 2019 u zaměstnanců povědomí o jejich povinnostech souvisejících s bezpečností ICT** **

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

**Graf 6.3: Firmy s 10 a více zaměstnanci v ČR se zkušeností s bezpečnostními incidenty v roce 2018** **

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

Zdroj: Český statistický úřad 2019