## 11. Bezpečnost informačního systému

Pojmem **bezpečnost informačního systému** se pro potřeby tohoto šetření rozumí měření, kontrola
a operace aplikované na informační systémy (dále IS) za účelem zajištění integrity, spolehlivosti, dostupnosti a důvěrnosti dat a systémů.

**Hacking** je činnost zaměřená na narušování počítačové bezpečnosti z různých důvodů (např. ze škodolibosti nebo k osobnímu prospěchu). Hackeři jsou osoby pronikající do zabezpečených sítí s úmyslem poškozovat data nebo vyřazovat sítě z provozu pro ostatní uživatele.

**Pharming, Phishing** jsou podvodné techniky používané k získávání citlivých údajů od obětí útoku. Principem pharmingu je napadení [DNS](https://cs.wikipedia.org/wiki/DNS) a přepsání [IP](https://cs.wikipedia.org/wiki/IP_adresa) adresy, čímž dochází k přesměrování klienta na falešné webové stránky předstírající portál [internetového bank](https://cs.wikipedia.org/w/index.php?title=Internetbanking&action=edit&redlink=1)ovnictví. Tyto stránky jsou obvykle
k nerozeznání od skutečných stránek [banky](https://cs.wikipedia.org/wiki/Banka). Cílem phishingu je získávání citlivých údajů ([hesel](https://cs.wikipedia.org/wiki/Heslo), čísel [kreditních karet](https://cs.wikipedia.org/wiki/Kreditn%C3%AD_karta) apod.) prostřednictvím [elektronické komunikac](https://cs.wikipedia.org/wiki/Telekomunikace)e.

**Denial of service** znamená techniku útoku na internetové služby nebo stránky, při níž dochází k přehlcení serverů požadavky a následnému zhroucení, omezení funkčnosti či nedostupnosti služeb ostatním uživatelům.

## Hlavní zjištění

* Formálně definovanou bezpečnostní politiku IS měla v České republice v lednu 2015 třetina podniků s deseti a více zaměstnanci. Vlastní bezpečnostní politiku mají stanovenou mnohem častěji velké podniky s 250 a více zaměstnanci (tři čtvrtiny z nich) než malé podniky (26 %). Bezpečnostní politiku měly vymezenou všechny velké podniky působící v oblastech Peněžnictví a pojišťovnictví, Telekomunikační činnosti a Ubytování. Vlastní bezpečnostní politika IS byla nejméně častá v podnicích v oboru Stravování a pohostinství či Maloobchodu (kromě motorových vozidel).
* Bezpečnostní politika IS pokrývá u necelé třetiny českých podniků (jedná se o více než 90 % těch, jež mají definovanou bezpečnostní politiku) rizika spojená se zničením či poškození dat v důsledku fyzického napadení popř. nečekaných událostí (živelná pohroma, požár, krádež, apod.).
* O něco více než čtvrtina podniků (resp. více než 80 % podniků s vlastní bezpečnostní politikou IS) je díky bezpečnostním pravidlům chráněna před riziky prozrazení důvěrných dat.
* Bezpečnostní politika IS pokrývá u čtvrtiny českých podniků (u více než dvou třetin podniků,
s definovanou bezpečnostní politikou) rizika znepřístupnění služeb systému z důvodu vnějšího útoku („Denial of service attack“).
* Před fyzickým útokem, vniknutím do systému (hacking, pharming, phishing atd.) a násilném získání důvěrných firemních dat, před vnějším útokem, kdy je systém úmyslně zahlcen požadavky a neschopen plnit svou funkci, jsou nejčastěji chráněny informační systémy podniků působících v oblasti IT a podniky z odvětví Peněžnictví a pojišťovnictví.
* Poslední nastavení případně redefinování bezpečnostní politiky ICT došlo u tří čtvrtin českých podniků v uplynulých 12 měsících. U necelé pětiny podniků před více než rokem ale před méně než 2 lety. Desetina podniků má bezpečnostní politiku starší než dva roky.

**Graf 11.1: Termín poslední revize/definování bezpečnostní politiky ICT v podnicích ČR\***

*\*podíl na celkovém počtu podniků s definovanou bezpečnostní politikou informačního systému (v %)*

**Tab. 11.1: Podniky s definovanou bezpečnostní politikou informačního systému, leden 2015**

|  |  |  |  |
| --- | --- | --- | --- |
|   | Celkem | Bezpečnostní potitika pokrývá rizika | Podniky, u nichž byla bezpečnostní politika IS revidována/definována |
| zničení či poškození dat | prozrazení důvěrných dat | vnějšího útoku do IS | v posledním roce | v posledních 12 až 24 měsících | před více než 2 roky |
| podíl na celkovém počtu podniků v dané velikostní a odvětvové skupině (%) | podíl na celkovém počtu podniků s definovanou bezpeč.politikou v dané velikostní a odvětvové skupině (%) |
| **Podniky celkem (10+)** | **33,4**  | **30,3**  | **27,5**  | **22,5**  | **75,6**  | **15,7**  | **8,7**  |
| **Velikost podniku** |   |   |   |   |   |   |  |
|  10–49 zaměstnanců | 26,2  | 23,0  | 21,3  | 16,8  | 78,3  | 14,0  | 7,7  |
|  50–249 zaměstnanců | 56,0  | 52,8  | 47,1  | 40,3  | 70,6  | 18,4  | 11,0  |
|  250 a více zaměstnanců | 74,7  | 71,9  | 60,1  | 54,0  | 74,2  | 18,3  | 7,5  |
| **Odvětví (ekonomická činnost)** |   |   |   |   |   |   |  |
|  Zpracovatelský průmysl | 33,6  | 30,9  | 25,6  | 19,6  | 70,0  | 18,1  | 11,9  |
|  Výroba a rozvod energie, plynu, tepla | 39,7  | 39,7  | 34,3  | 27,9  | 78,6  | 14,5  | 7,0  |
|  Stavebnictví | 23,8  | 20,1  | 20,6  | 17,8  | 82,0  | 8,1  | 9,9  |
|  Obchod; opravy motorových vozidel | 33,6  | 29,0  | 28,0  | 23,9  | 75,2  | 17,5  | 7,3  |
|  Doprava a skladování | 23,0  | 20,8  | 16,2  | 15,0  | 69,6  | 19,9  | 10,5  |
|  Ubytování, stravování a pohostinství | 17,1  | 15,7  | 15,4  | 12,5  | 77,0  | 14,6  | 8,3  |
|  Informační a komunikační činnosti | 68,7  | 65,9  | 61,2  | 52,7  | 78,2  | 14,8  | 7,0  |
|  Peněžnictví a pojišťovnictví | 77,6  | 69,7  | 64,4  | 60,3  | 82,6  | 14,3  | 3,1  |
|  Činnosti v oblasti nemovitostí | 35,2  | 32,9  | 28,5  | 26,1  | 72,5  | 21,3  | 6,2  |
|  Profesní, vědecké a technické činn. | 47,0  | 43,5  | 40,1  | 30,5  | 81,9  | 10,8  | 7,3  |
|  Administrativní a podpůrné činnosti | 35,5  | 32,9  | 32,6  | 24,8  | 87,2  | 11,6  | 1,2  |

**Graf 11.2: Podniky\* s formálně definovanou bezpečnostní politikou informačního systému**

**Graf 11.3: Podniky\*, jejichž bezpečnostní politika pokrývá následující rizika:**

*\*podíl na celkovém počtu podniků v dané velikostní a odvětvové skupině (v %)*

*Zdroj: Český statistický úřad 2015*