

530 útoků hackerů na české firmy každý týden, více než kdekoli na světě! Nejvíce útoků přichází z USA!

- CZ24 News | 26. května 2020

ČESKO: Na české firmy a organizace připadne 530 útoků za týden, celosvětový průměr je přitom 491. Po poklesu útoků na začátku roku jejich počet nyní znovu roste. Škodlivé soubory se do českých organizací snaží nejčastěji dostat prostřednictvím webových stránek. Hackeri se zaměřují stále více na cílené útoky, které mají vyšší šanci na úspěch.

Česko je nad světovým průměrem v počtu kybernetických útoků na místní firmy a organizace. Zatímco na české organizace připadá 530 útoků za týden, celosvětový průměr je 491 útoků.

Po pozvolném poklesu útoků na začátku roku jejich počet v poslední době opět roste. Vyplývá to z dat bezpečnostní společnosti Check Point za uplynulých šest měsíců.

Nejčastějším zdrojem kybernetických hrozeb pro české organizace jsou Spojené státy, ze kterých pochází 33 procent hrozeb, 22 procent je od domácích hackerů, 17 procent pochází z Irska, osm procent z Nizozemska, sedm z Německa a pět procent ze Španělska.

Z 92 procent se škodlivé soubory do českých organizací snaží dostat prostřednictvím webových stránek, prostřednictvím e-mailů distribuují útočníci pouze osm procent z nich. V celosvětovém měřítku je přes webové stránky distribuováno jen 36 procent škodlivých souborů, zatímco 64 procent je šířeno e-maily.

Škodlivé soubory distribuované v e-mailech jsou nejčastěji soubory s koncovkou .exe, ale jejich podíl proti polovině minulého roku klesl z 50 procent na 36 procent. Na druhé místo se posunuly škodlivé soubory s koncovkou .xlsx. Celosvětovému žebříčku vévodí také formát .exe (35,1 procenta škodlivých souborů distribuovaných e-maily), ale na druhé příčce je s výrazným podílem formát .xls.

U škodlivých souborů distribuovaných prostřednictvím webových stránek je situace v Česku jednoznačná. Na 98 procent takových souborů má koncovku .pdf. Ve světě má třetina škodlivých souborů koncovku .exe a víc než pětina .pdf.

Vyděračský ransomware dlouhodobě ovlivňuje méně než procento českých společností, ale je to způsobené taktikou kybernetických zločinců.

„Zaměřují se stále více na cílené útoky, které mají vyšší šanci na úspěch. Navíc útoky jsou nebezpečnější a často se setkáváme s dvojitým vydíráním. Útočníci požadují nejenom výkupné za dešifrování dat, ale hrozí i zveřejněním ukradených informací. Výkupné postupně zvyšují a na speciálních webových stránkách nabízí zcizená data, dokud nejsou splněné jejich požadavky,“ uvedl expert Check Pointu Pavel Krejčí.

Od poloviny března zaznamenal Check Point výrazný nárůst útoků tzv. botnetů, tedy sítí ovládaných počítačů. Do té doby ovlivňovaly zhruba pět procent českých společností, ale během měsíce vzrostl jejich dopad až na téměř 15 procent. Lehce začaly růst útoky programů těžících kryptoměny a bankovních škodlivých kódů.