TISKOVÁ ZPRÁVA 31. 8. 2021

**Podle průzkumu společnosti Accenture se frekvence kybernetických útoků v první polovině roku 2021 více než zdvojnásobila**

Jak ukazuje nejnovější průzkum oddělení Cyber Investigations, Forensics & Response (CIFR) společnosti Accenture, ve srovnání se stejným obdobím loňského roku se v první polovině roku 2021 množství kybernetických útoků celosvětově zvýšilo o 125 %. Informace je odvozená na základě přímé spolupráce se zákazníky v rámci jejich reakce a zotavení se z incidentů v kyberprostoru.

Trojciferný nárůst (o 125 %) byl způsoben především nedostatečným zabezpečením vzdáleného přístupu k webovým serverům (web shell) a následným spuštěním škodlivého kódu s cílem získání přístupu a kontroly. Příklady zahrnují použití cíleného ransomware a následného vydírání či narušení a zneužití dodavatelského řetězce.

„Z hlediska oborů byl nejčastěji zasažen sektor spotřebního zboží a služeb představující 21 % kybernetických útoků, dále následují průmyslový/výrobní sektor (16 % útoků), bankovní sektor (10 % útoků) a sektor cestovního ruchu a gastroprůmysl (9 %),“ přibližuje výsledky průzkumu Michal Merta, odborník na informační bezpečnost a ředitel pražského Cyber Fusion Centra Accenture.



Více než 70 % incidentů zaznamenaných CIFR týmem směřovalo na tři státy, a to na USA (36 %), Velkou Británii (24 %) a Austrálii (11 %).

„Mnoho organizací dnes zabezpečuje pouze hlavní podnikové systémy a nechrání svůj dodavatelský řetězec, dceřiné a přidružené společnosti. Proto je klíčové mít ucelený plán na pokrytí celého IT ekosystému,“ říká Michal Merta, a dodává: „Společnosti působící v odvětvích jako spotřební zboží a služby, průmysl, maloobchod, cestovní ruch a pohostinství, jež během pandemie zaznamenávaly spíše nižší počet kybernetických útoků, by měly revidovat svou současnou úroveň zabezpečení, neboť zvýšená aktivita spotřebitelů v těchto odvětvích představuje nové příležitosti pro útočníky.“

Průzkum také podrobně popisuje nejčastější kategorie malware, jednotlivé varianty ransomware a odvětví, na která se útoky v první polovině roku 2021 zaměřovaly nejčastěji. Zde jsou klíčová zjištění:

* Nejčastější používaný malware byl typu ransomware (38 %), hned poté následovaly pokusy o získání neoprávněného přístupu (33 %).
* Revil/Sodinokibi byl nejčastěji pozorovaný druh ransomware – představoval 25 % incidentů.
* Ransomware útoky nejčastěji cílily na oblasti pojišťovnictví (23 % útoků), spotřebního zboží a služeb (17 %) a na telekomunikace (16 %).
* Společnosti s ročními tržbami 1–10 miliard USD představovaly více než polovinu (54 %) obětí ransomware a vydírání, následovaly společnosti s ročními tržbami mezi 10 miliardami a 20 miliardami USD (20 %).

„U větších společností je dopad kybernetického útoku významnější a také se v jejich případě častěji mluví o úniku citlivých dat. Proto jsou takové útoky veřejnosti více známy a mnohdy se o nich můžeme dozvědět z médií. To ale neznamená, že menší společnosti nejsou pro útočníky lákavým cílem, právě naopak. Jen se o tom tolik nepíše,“ uzavírá Michal Merta.

**O společnosti Accenture**

Accenture je globální společnost poskytující profesionální služby v oblasti digitalizace, cloudu a kybernetické bezpečnosti. Díky propojení zkušeností a specializovaných dovedností ve více než 40 průmyslových odvětvích nabízíme služby v oblastech poradenství & strategie, Interactive, Technology a Operations – a to díky podpoře největší celosvětové sítě Advanced Technology a Intelligent Operations center. Našich 567 000 zaměstnanců využívá možnosti nejnovějších technologií i lidské vynalézavosti v práci pro klienty ve více než 120 zemích. Díky síle změn vytváříme hodnoty a zvyšujeme úspěšnost našich klientů, lidí, akcionářů, partnerů i celé společnosti. Navštivte nás na [www.accenture.com](http://www.accenture.com/) nebo <https://www.accenture.com/cz-en/about/company/newsroom>.

**Kontakt pro média:** Lukáš Vejnar, lukas.vejnar@accenture.com, 605 067 979

Petr Jarkovský, petr.jarkovsky@aspen.pr, 774 225 153

 Markéta Ciňková, marketa.cinkova@aspen.pr, 724 012 612