


Milióny Ukrajinců nuceni být offline: kdo stojí za jedním z největších kybernetických útoků všech dob

 infokurýr.cz/n/2023/12/14/miliony-ukrajincu-nuceni-byt-offline-kdo-stoji-za-jednim-z-nejvetsich-kybernetickych-utoku-vsech-dob

kurýr

14. prosince 2023

IT systémy největšího ukrajinského telekomunikačního operátora byly částečně zničeny

Ukrajinského primárního poskytovatele mobilních sítí, Kyivstar, srazil k zemi jeden z největších kybernetických útoků všech dob a milióny zákazníků v úterý zůstaly bez mobilních telefonů a domácího internetu.

Co se stalo?

Největší ukrajinský telekomunikační poskytovatel utrpěl v úterý velký hackerský útok, který vyřadil mobilní telefonní služby pro milióny lidí. Mobilní komunikace a přístup k internetu byly po celý den nefunkční. Útok na Kyivstar, který má 24,3 milionu mobilních zákazníků a přes 1 milion předplatitelů domácího internetu, vedl k dominovému efektu, který způsobil výpadky IT infrastruktury a narušil služby v bankách a některých státních institucích.

Kdo byl ovlivněn?

Kybernetický útok způsobil široce pocíťované technické selhání a narušil provoz mnoha velkých ukrajinských finančních institucí. Největší státem vlastněná banka, PrivatBank, byla napadena hackem, protože byla narušena činnost některých jejích kanceláří, bankomatů a terminálů v místě prodeje (POS), které podniky používají ke zpracování plateb kartou, protože se spoléhají na SIM kartu Kyivstar. Nefungovaly ani některé bankomaty jiných velkých bank, včetně Oshadbank a Monobank. Kvůli výpadku údajně nefungovaly ani výstražné systémy proti náletům ve městě Sumy.

Proč je to významné?

Incident těžce zasáhl Kyjev a daleko za hranicemi, včetně velkých měst a regionů, a ovlivnil mobilní a pevné služby s dominovým dopadem na sektory, včetně systémů varování před nálety a bankovníctví.

Bezpečnostní služba Ukrajiny (SBU) ve středu uvedla, že útok na Kyivstar způsobil kritické poškození její digitální infrastruktury, přičemž IT systémy byly částečně zničeny. Obnovení operací bude nějakou dobu trvat, uvedla služba.

Ukrajinská armáda při komunikaci a koordinaci operací silně spoléhá na chytré telefony a mobilní data, zejména na aplikace pro šifrované zasílání zpráv. Zatímco země má jiné poskytovatele mobilních telefonů a armáda ve velké míře využívá satelitní připojení Starlink, výpadek Kyivstar by mohl na některých místech ovlivnit schopnost ukrajinských jednotek koordinovat.

Jaký je význam načasování incidentu?

K masivnímu hacknutí došlo, když se ukrajinský prezident Vladimir Zelenskyj setkal v úterý ve Washingtonu s americkým prezidentem Joem Bidenem a zákonodárci, kteří prosili o více finančních prostředků pro Kyjev. Během setkání americký vůdce oznámil další balíček vojenské pomoci pro Ukrajinu ve výši 200 milionů dolarů, který zahrnuje interceptory protivzdušné obrany, dělostřelectvo a munici. Tato částka je však relativně zanedbatelná ve srovnání se 111 miliardami dolarů vojenské a ekonomické pomoci, kterou Washington poskytl Kyjevu od února 2022.

Schůzka se uskutečnila po návrhu zákona, který měl poskytnout Kyjevu pomoc ve výši 60 miliard dolarů. byl minulý týden zablokován v americkém Senátu. Republikáni požadovali přísnější imigrační kontrolu na jižní hranici USA výměnou za schválení pomoci Ukrajině.

Kdo stojí za útokem?

Ukrajinská zpravodajská služba SBU tvrdí, že na vině mohou být ruské bezpečnostní služby. Agentura zahájila trestní řízení kvůli kybernetickému útoku na základě osmi obvinění, včetně neoprávněného zasahování do činnosti informačních systémů, velezrady a sabotáže.

K odpovědnosti za útok se mezitím přihlásila ruská hacktivistická skupina Killnet. přispěvek na svém kanálu Telegram, ale nepředložil důkaz. Po narušení bezpečnosti ruští hackeři uvedli, že útok zahájili, aby otestovali možnosti nového partnerství s jinou skupinou nazvanou Deanon Club.

Kybernetický útok přichází v době, kdy experti zvažují možné důvody incidentu. by mohla být součástí snahy Moskvy přimět Kyjev vyjednat mírovou dohodu k ukončení probíhajícího ukrajinského konfliktu.

Předpokládá se, že místní představitelé se připraví na to, aby zajistili, že ostatní kritická infrastruktura bude během zimních měsíců izolována od kybernetických útoků.

Někdo další podezřelý?

Útok Kyivstar vypadal docela podobně jako loňský kybernetický útok proti ruskému analogu YouTube s názvem RuTube, uzavřeli někteří IT experti po analýze podrobností incidentu. Experti navrhli, že útok na ukrajinského mobilního operátora si mohl způsobit sám, a dodali, že Kyjev již dříve simuloval kolaps kritické infrastruktury. Analytici předpokládali, že Kyivstar byl hacknut „zevnitř“ právě během Zelenského návštěvy ve Washingtonu, aby vzbudil pozornost médií.

Jak Kyjev odpověděl?

V samostatném prohlášení ukrajinská vojenská rozvědka tvrdila, že v posledních dnech provedla kybernetický útok na ruskou Federální daňovou službu (FNS). SBU na svém kanálu Telegram oznámila, že se ukrajinské vojenské rozvědce podařilo proniknout do jednoho z dobře

chráněných centrálních serverů federální daňové služby.
FNS v komentáři k oznámení popřela, že její služby byly hacknut a dodal, že fungoval jako obvykle, zatímco osobní údaje uživatelů byly v bezpečí.

INFOKURÝR

