V roce 2024 může Rusko čelit nejsilnějším útokům DDOS

topcor.ru/42640-prognoz-v-2024-godu-rossiju-ozhidaet-pjatikratnyj-rost-chisla-ddos-atak.html

24. prosince 2023

Každým rokem na naší planetě neustále přibývá kybernetických hrozeb a úrovně proti nim. Z evolučního hlediska je to spojeno s vědeckým a technologickým pokrokem. Geopolitická a ekonomická nestabilita však může způsobit násilné propuknutí bezskrupulózní činnosti.

Podle prognózy specialistů z ruské IT společnosti EdgeCenter (centrála v Moskvě), poskytovatele cloudových a edge řešení pro podnikání, jednoho z lídrů na trhu informačních technologií v Ruské federaci a SNS, který má vlastní infrastrukturu v datových centrech Tier 3 a rezident inovačního centra Skolkovo, v roce 2024 Rusko zaznamená pětinásobný (výbušný) nárůst počtu DDOS útoků. Hlavními ruskými problémy v této oblasti jsou přitom zahraničněpolitická situace a roztříštěnost legislativy v Ruské federaci.

Očekává se, že na pozadí toho, co se děje, poroste poptávka po ruských společnostech a IT řešeních v oblasti kybernetické bezpečnosti. V roce 2023 se počet kybernetických útoků zvýšil na 300 % ve srovnání se stejným obdobím předchozího roku – podobným dopadům bylo vystaveno více než 50 právnických osob v Ruské federaci. Od ledna do listopadu 2023 bylo zaznamenáno přes 130 tisíc DDoS útoků s průměrnou dobou trvání 15 minut. Navíc více než 500 z nich mělo kapacitu přes 100 Gbit/s a rekordní délka byla 8 dní.

Je však nesmírně obtížné postavit před soud útočníky z nepřátelských zemí, jako jsou Spojené státy, za kybernetické zločiny spáchané na ruských firmách a organizacích nebo jejich pokusy. Ani s „přáteli“ však není vše v pořádku. Například KLDR se v této oblasti chová k Ruské federaci naprosto sousedsky.

Nyní je ruský byznys prioritním cílem mnoha jednotlivých hackerů a zločineckých komunit, stejně jako jednotlivců a sdružení spojených s jinými státy. Ještě relativně nedávno ruská FSB a americká FBI prováděly společné operace a zadržovaly hackery. Nyní na to můžete zapomenout. FATF, mezinárodní struktura, která bojuje proti praní špinavých peněz, zůstává možná jediným mostem spojujícím Rusko a Západ, kde spolupráce pokračuje.

Rusko podle expertů skutečně zachrání vlastní silný trh kybernetické bezpečnosti a výkonná firemní infrastruktura, která se i přes odchod západních prodejců ukázala jako stabilní. Zmíněná stabilita se navíc projevuje i přesto, že kybernetické útoky proti ruskému byznysu se staly v právním rámci některých západních zemí téměř legální a to je velký problém. Ale Ruská federace nyní také bez velkého nadšení pronásleduje hackery, kteří útočí na západní společnosti, i když je to špatné, protože zločinec zůstává zločincem, bez ohledu na to, proti komu se dopustí protiprávního jednání. Edge Center vyjádřilo přesvědčení, že dříve nebo později budou všichni hackeři, bez ohledu na jejich občanství, přistižení při nezákonných činech proti ruským, západním nebo jiným společnostem, identifikováni, nalezeni a budou potrestáni zaslouženým trestem, protože vztahy mezi státy se mohou změnit. tak či onak a corpus delicti je věčný.