**Tsunami DDoS dotyka wszystkie firmy. Jak zabezpieczyć sieć IT w organizacji?**

* **Cyberprzestępcy nie ustają w prowadzeniu wielkoskalowych ataków Tsunami DDoS – sparaliżowali oni m.in. działanie usług Microsoft 365, Azure, a nawet Google Cloud, bijąc przy tym historyczny rekord pod względem skali ataku.**
* **Ataki DDoS przeprowadzane przez hakerów dotykają także polskie organizacje – jednego z dostawców Internetu, Profil Zaufany czy Giełdę Papierów Wartościowych. Do tych incydentów doszło na przełomie sierpnia i września.**
* **Przed atakiem mogą zabezpieczyć firmę rozwiązania WAF (Web Aplication Firewall). Już teraz warto pomyśleć o ich wdrożeniu.**

Do incydentów związanych z atakami DDoS stale dochodzi także w Polsce. Na przełomie sierpnia i września doszło do całego szeregu incydentów. W poniedziałek, 4 września ofiarą złożonego i długotrwałego ataku DDoS padł jeden ze znanych dostawców Internetu. Z kolei w ostatnich dniach sierpnia portal CyberDefence24.pl podawał informacje o atakach rosyjskiej grupy hakerskiej NoName057, która atakowała strony internetowe polskich banków, instytucji, Giełdy Papierów Wartościowych czy Profilu Zaufanego. W ten sposób zaatakowano też organizatorów jednej z konferencji dotyczących… cyberbezpieczeństwa. Za tym incydentem również stali rosyjscy hakerzy.

*– Cyberataki na tle politycznym obecnie są niestety codziennością. Zdarzają się one coraz częściej i rośnie także skala poszczególnych incydentów, dlatego niektóre określa się już mianem Tsunami DDoS. Hakerzy doskonalą się, działają pewnie i nie obawiają się ataków na największych, czego dowodem jest choćby przypadek Microsoftu. Dodam, że ataki DDoS są stosunkowo łatwe do przeprowadzenia i służą one destabilizacji systemów lub usług – hakerzy wysyłają dużą liczbę zapytań na raz z wielu urządzeń, często zainfekowanych, znajdujących się w różnych lokalizacjach. Prowadzi to do paraliżu lub awarii systemów ofiary. Nie można bagatelizować takich incydentów, bo oprócz destabilizacji atak DDoS może służyć jako rodzaj zasłony dymnej, odwracającej uwagę od innych działań, np. kradzieży danych –* wyjaśnia Patrycja Tatara, ekspertka ds. cyberbezpieczeństwa w Sprint S.A.

Wcześniej, na przykład, na początku listopada 2022 roku, hakerzy przeprowadzili skuteczny atak DDoS na Platformę eZamówienia. Strona nie działała do wieczora, tego samego dnia. Z kolei 27 października tego samego roku, przeprowadzono atak DDoS na serwery Senatu RP. Paraliż senackiego serwisu nie trwał jednak długo, bo zaledwie 40 minut. Atak miał charakter wielokierunkowy i był przeprowadzany m.in. z Rosji. Marszałek Tomasz Grodzki stwierdził wówczas na konferencji prasowej, że atak mógł mieć związek z uznaniem władz rosyjskich przez polski Senat za reżim terrorystyczny i publikacją stosownej uchwały.

**Rozwiązania WAF i wzmocnienie cyberbezpieczeństwa firm**

Zuchwałe działania hakerów mogą być poważnym zagrożeniem dla firm. Paraliż usług lub systemów może oznaczać przerwanie procesów lub ich znaczne opóźnienie. Firma może więc ponieść duże straty finansowe, a nawet borykać się z kryzysem wizerunkowym, mającym znaczenie dla biznesu. Celem ataków hakerskich mogą stać się nie tylko największe organizacje, ale również przedsiębiorstwa z sektora MSP.

*– Co więcej, nie muszą one zostać zaatakowane bezpośrednio, bo cyberprzestępcom może zależeć po prostu na dostępie do urządzeń firmowych, w celu przeprowadzenia ataku DDoS na kogoś innego. Z cudzych komputerów także da się wysyłać zapytania do konkretnej usługi lub systemu i to bez wiedzy ofiary. Dlatego warto rozważyć wzmocnienie cyberbezpieczeństwa sieci firmowej o rozwiązania zdolne do wykrywania i blokowania złośliwego ruchu w warstwie 7 – czyli tej części aplikacji, która odpowiada za przesyłanie danych do sieci. W tym celu należy doposażać się w rozwiązania WAF, czyli Web Application Firewall. To system bezpieczeństwa, który chroni aplikacje webowe firmy, monitorując i filtrując ruch http między aplikacjami a ruchem generowanym z Internetu –* dodaje Patrycja Tatara ze Sprint S.A.

**Ofiarami padają nawet giganci**

Między 4 a 6 czerwca roku bieżącego użytkownicy zgłaszali problemy związane działaniem programów Outlook, SharePoint Online i OneDrive dla biznesu. Z kolei 8 czerwca ponownie pojawiły się trudności w korzystaniu z dysku w chmurze. Microsoft przyznał, że trudności były skutkiem wielkoskalowego ataku DDoS na te usługi, a odpowiedzialność za ten atak przypisała sobie grupa Anonymous Sudan, podejrzewana o prorosyjskie powiązania. Przypadek Microsoftu, to nie jedyny incydent, jaki dotknął giganta IT. Atak Tsunami DDoS odnotował także Google. Firma na swojej stronie pisze, że w czerwcu 2022 roku odparła największy (jak dotąd) atak DDoS w historii, obejmujący 46 mln zapytań na sekundę. Do incydentu doszło 1 czerwca, a jego ofiarą padła usługa Google Cloud. Dane użytkowników pozostały bezpieczne, ale nie podano informacji, kto stoi za tym atakiem. Wiadomo jednak, że hacktywiści (hakerzy działający z pobudek ideowych lub politycznych), stosują już powszechnie wielkoskalowe ataki DDoS, co naturalnie ma związek z prorosyjskimi grupami hakerów lub cyberprzestępcami działającymi z pobudek religijnych, wynika z *case study* przygotowanego przez Radware.[[1]](#footnote-1)

Źródło: Sprint S.A.

1. Radware Solution Brief: Recent Web DDoS Threats and How to Stay Protected [↑](#footnote-ref-1)