CLOUDFLARE

Kod czerwony: Ataki DDoS zagrażają bezpieczeństwu pacjentów

Opieka zdrowotna pozostaje głównym celem ataków DDoS (Distributed Denial-of-Service). Przytłaczając krytyczne systemy, ataki te powodują maksymalne zakłócenia, co skutkuje zablokowaniem dostępu do rekordów EHR, systemów do zarządzania i nie tylko. To nie tylko przestoje; stanowi to bezpośrednie zagrożenie dla opieki i bezpieczeństwa pacjentów.

70%

Większość organizacji opieki zdrowotnej (70%) borykała się z umiarkowanymi do poważnych skutkami finansowymi incydentów cybernetycznych[1].

10,93 mln USD

W porównaniu z innymi branżami opieka zdrowotna ma najwyższy średni koszt naruszenia bezpieczeństwa i wynosi 10,93 mln USD.2

#1

Opieka zdrowotna jest sektorem będącym największym celem ataków z wykorzystaniem oprogramowania typu ransomware[3], w tym ataków DDoS z okupem.

59%

W ponad połowie (59%) organizacji opieki zdrowotnej cybernincydent opóźnił leczenie, nadszarpnął zaufanie pacjentów lub spowodował inne wyzwania kliniczne[4].

Dodatkowy efekt ataków DDoS

Ataki DDoS złośliwie zalewają serwer, usługę lub sieć „śmieciowym" ruchem internetowym. Ich celem jest przytłoczenie i wyłączenie usług online, co będzie miało wpływ na cały ekosystem opieki zdrowotnej:

Paraliż związany z opieką nad pacjentem: Ataki na portale, telezdrowie i raporty EHR powodują zablokowanie personelu i blokują dostęp pacjentów do kluczowych usług.

Zasłona dymna związana z naruszeniem bezpieczeństwa danych: Ataki DDoS często rozpraszają i przytłaczają zespoły ds. bezpieczeństwa, zapewniając przykrywkę przed jednoczesną kradzieżą bardzo cennych danych pacjentów (PHI).

Zakłócenia łańcucha dostaw: ataki mogą wstrzymać badania kliniczne, wysyłki leków oraz operacje finansowe, takie jak roszczenia i wstępne autoryzacje.

Plan postępowania: cztery niezbędne zabezpieczenia przed atakami DDoS

1 **Widoczność i zróżnicowanie:** Podobnie jak leki, które blokują sygnały bólowe, a jednocześnie umożliwiają Twojemu organizmowi funkcjonowanie, Twoje rozwiązanie DDoS musi blokować tylko ataki, a nie „zdrowy" ruch.

2 **Skala globalna:** sieć w chmurze o nieograniczonej pojemności może wchłonąć największe ataki, zapewniając jednocześnie szybkie i bezpieczne działanie portali EHR, aplikacji m-zdrowia oraz innych usług cyfrowych.

4 **Ochrona dla każdego połączenia:** Ochrona przed atakami DDoS w aplikacjach i sieciach dostępnych na zewnątrz jest kluczową pierwszą linią obrony. Jeśli jednak atak się powiedzie, ochrona w modelu Zero Trust może zapobiec naruszeniom systemów wewnętrznych i danych.

3 **Obrona adaptacyjna**— im większa i bardziej niezawodna sieć łagodząca, tym więcej informacji może dostarczyć w odniesieniu do zmieniających się wzorców ataków. Pomaga to zwiększyć „odporność" na przyszłe ataki.

Zapobiegaj ograniczaniu najbardziej zaawansowanych ataków DDoS

> Łatwość użycia Cloudflare, automatyczne aktualizacje i automatyczna ochrona przed zagrożeniami pozwalają nam zaoszczędzić czas i siłę roboczą, jednocześnie pozwalając nam utrzymać wysoki poziom cyberbezpieczeństwa przed zagrożeniami, które mogą zaszkodzić naszym pacjentom i naszej firmie.
>
> **Wisut Ua-Anant**
> Chief Digital MarTech Officer
> Bumrungrad International HOSPITAL

Przeczytaj ich historię

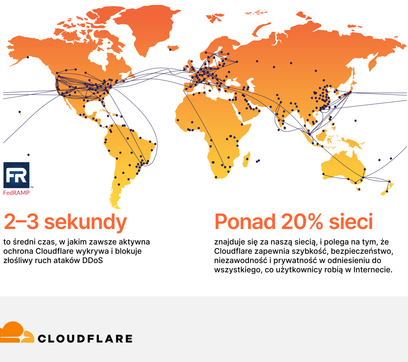
Zintegrowana ochrona przed atakami DDoS warstw L3–7 monitoruje, zapobiega i łagodzi ataki, zanim zaszkodzą Twojej organizacji lub opiece nad pacjentem.

234 mld cyberzagrożeń

są blokowane (średnio) przez Cloudflare każdego dnia[4]

449 Tb/s przepustowości

sprawia, że Cloudflare jest w stanie zaabsorbować największe ataki DDoS — w tym największy na świecie atak DDoS5 — rekordowe 29,7 Tb/s.



FedRAMP

2–3 sekundy

to średni czas, w jakim zawsze aktywna ochrona Cloudflare wykrywa i blokuje złośliwy ruch ataków DDoS

Ponad 20% sieci

znajduje się za naszą siecią, i polega na tym, że Cloudflare zapewnia szybkość, bezpieczeństwo, niezawodność i prywatność w odniesieniu do wszystkiego, co użytkownicy robią w Internecie.

CLOUDFLARE

Zwiększ ochronę przed atakami DDoS i innymi zagrożeniami, płynne doświadczenia pacjentów oraz zwiększ zgodność z przepisami — wszystko to dzięki jednej, bezpiecznej platformie chmurowej Cloudflare.

Dowiedz się, jak to zrobić

Źródła:

1. Emily Olsen, ankieta „Most care Dive" z 6 listopada 2025 r.
2. Mike Elgan, „Cost of a data connectivity: The care care", IBM, udostępniony przez IBM z 6 listopada 2025 r.
3. Steve Alder, „Q1 2025 Ransomware Report", The HIPAA Journal, 10 kwietnia 2025 r.
4. Stan na 3. kwartał 2025 r. (źródło: Cloudflare)
5. Stan na październik 2025 r. (źródło: Cloudflare)