[TLP:WHITE]

Dobre praktyki w zakresie przeciwdziałania atakom DDoS

Warszawa
Luty 2022

Spis treści

I. Wstęp

Współczesna Organizacja działająca w nowoczesnym i dynamicznym otoczeniu gospodarczym uzależniona jest w dużym stopniu od domeny cyfrowej, w której powinna funkcjonować w sposób bezpieczny, z zachowaniem zasad poufności, integralności oraz dostępności.

Jednym z popularnych rodzajów działań cyberprzestępców wymierzonych w atrybut dostępności są ataki na tzw. odmowę usługi (ang. *Denial of Service*, DoS) oraz *Distributed Denial of Service* (DDoS)[1].

W uproszczeniu, ataki DDoS można scharakteryzować jako ataki powodujące czasową niedostępność systemów teleinformatycznych i usług Organizacji świadczonych drogą elektroniczną. Często ataki DDoS bezpośrednio wpływając na atrybut dostępności powodują również wpływ na atrybuty integralności oraz poufności danych, generując wysokie ryzyko ich utraty przez Organizację.

Brak dostępności spowodowany atakami DDoS może doprowadzić do materializacji szeregu istotnych ryzyk po stronie Organizacji, takich jak np.:

a) znaczne straty finansowe wynikające z braku ciągłości prowadzenia działań biznesowych, a co za tym idzie roszczeń klientów oraz zewnętrznych dostawców, odbiorców usług itd.;
b) straty wizerunkowe wynikające z czasowego braku realizacji usług dla klientów biznesowych oraz indywidualnych;
c) naruszenie przepisów prawa;
d) inne, bliżej nie zdefiniowane ryzyka materializujące się w przypadku niedostępności usług.

Niedostępność usług Organizacji (lub w skrajnym przypadku kilku albo więcej Organizacji z jednego lub kilku sektorów gospodarki), która w wyniku ataku nie będzie w stanie świadczyć swoich usług, może mieć też znaczący, negatywny wpływ na ogólną sytuację społeczno-gospodarczą w kraju jeżeli:

a) Organizacja świadczy usługi publiczne dla obywateli;
b) Organizacja jest instytucją zaufania publicznego;
c) Organizacja świadczy usługi tzw. pierwszej potrzeby;
d) Organizacja realizuje usługi niezbędne do funkcjonowania społeczeństwa;
e) Organizacja świadczy usługi dla szerokiego grona innych Organizacji realizujących powyższe zadania (*chain of supply*);
f) Organizacja dostarcza usługi dla kluczowych podmiotów odpowiedzialnych za szeroko pojęte bezpieczeństwo.

[1] Dla uproszczenia w dalszej części opracowania używane jest określenie DDoS.

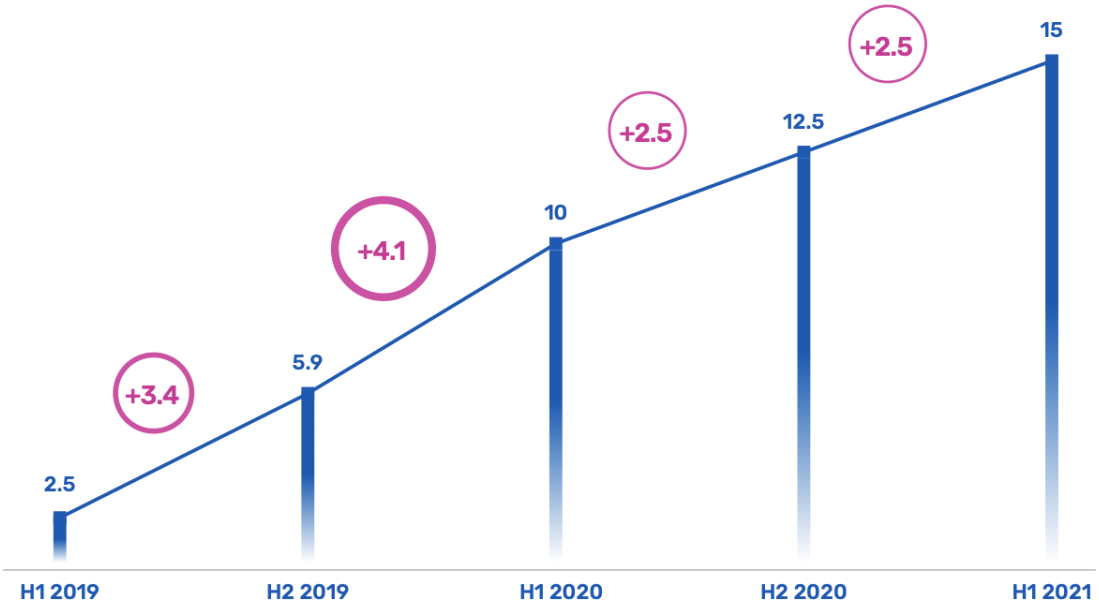
Poziom zaawansowania oraz skuteczność ataków DDoS drastycznie wzrosły, stając się często elementem oferowanego przez przestępców modelu CaaS (*Cybercrime as a Service*). Gotowe do użycia usługi umożliwiające przeprowadzenia ataków DDoS dostępne sią już nie tylko w DarkNecie, ale również bezpośrednio w sieci Internet, reklamowane na kanałach Youtube lub na portalu Reddit. Zgodnie z przewidywaniami firm analizujących ataki DDoS w skali globalnej, ich skala będzie rosła m.in. przez wdrażanie technologii 5G umożliwiającej podłączanie do sieci Internet nowych urządzeń, popularyzacji tzw. internetu rzeczy (ang. *Internet of Things*, IoT) (która oznacza, że znacznie więcej urządzeń jest wpiętych do sieci IP), rozwojowi sieci światłowodowych dla użytkowników końcowych czy ogólnemu wzrostowi liczby i przepustowości łączy internetowych użytkowników końcowych.

Zgodnie ze statystykami zawartymi w raporcie ENISA[2] z 2019 r.:

- łączna liczba ataków DDoS w III kwartale 2019 r. (w porównaniu z analogicznym okresem 2018 r.) wzrosła o 241%;
- 79,7% wszystkich ataków DDoS to SYN-Floods;
- 86% zmitygowanych ataków w III kwartale 2019 r. korzystało z więcej niż dwóch wektorów;
- 84% ataków DDoS trwało mniej niż 10 minut;
- najdłuższy atak DDoS w II kwartale 2019 r. trwał 509 godzin.

Poniżej przedstawiono przykładowe statystyki dot. rosnącej skali ataków DDoS opublikowane przez:

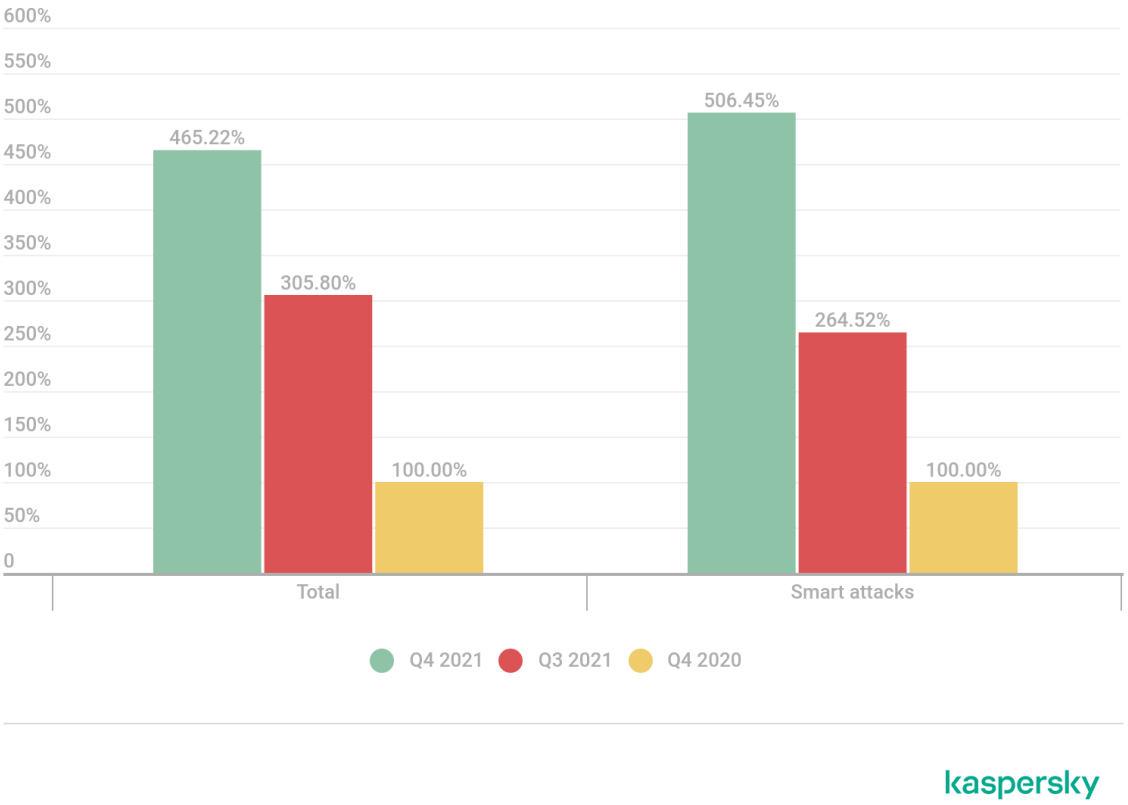
a) firmę A10 za I kwartał 2021 r. (skala w mln)



Rys. 1 – wzrost skali ataków DDoS na przestrzeni lat 2019-2021. Źródło[3].

[2] Źródło: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service
[3] Źródło: https://www.a10networks.com/wp-content/uploads/A10-EB-ddos-attack-mitigation-a-threat-intelligence-report.pdf

b) firmę Kaspersky porównującą skalę ataków DDoS pomiędzy Q4 2020 (przyjęte jako 100%) a Q3 i Q4 2021 r., która wskazuje wzrosty od ~250 do ~500%



Rys. 2 – wzrost skali ataków DDoS Q4 2020 – Q3, Q4 2021. Źródło[4].

Ataki DDoS stają się nie tylko narzędziem działań cyberprzestępców (rozumianych jako grupy cyberprzestępcze) zorientowanych na zysk finansowy[5], ale są wykorzystywane też przez tzw. *state sponsored hackers* tj. grupy hakerskie działające w strukturze lub na zlecenie poszczególnych państw.

Będąc faktyczną bronią ofensywną działającą w cyberprzestrzeni stają się elementem nacisku i bezpośredniego wpływu w rozgrywkach geopolitycznych.

Opracowanie poprzedzone niniejszym wstępem jest wynikiem prac specjalistów z zakresu telekomunikacji i cyberbezpieczeństwa i przedstawia zbiór dobrych praktyk zestawionych z koncepcjami rozwiązań dotyczących architektury telekomunikacyjnej, które powinny być poddane wnikliwej analizie przez każdą Organizację.

[4] Źródło: https://securelist.com/ddos-attacks-in-q4-2021/105784/
[5] Źródło: https://www.proofpoint.com/us/blog/threat-insight/ransom-ddos-extortion-actor-fancy-lazarus-returns

Z praktycznych względów opracowanie nie zawiera charakterystyki rodzajów ataków DDoS – wszystkie niezbędne informacje są publicznie dostępne w sieci Internet, a działania cyberprzestępców w tym obszarze stale ewoluują, co w krótkiej perspektywie czasowej doprowadziłoby do dezaktualizacji opracowania.

Przedstawione w opracowaniu koncepcje, narzędzia i techniki chroniące przed atakami DDoS celowo nie są przypisane do konkretnych rodzajów ataków, gdyż niejednokrotnie zastosowanie jednego z tych rozwiązań pozwala na ochronę przed różnymi rodzajami ataków na odmowę usługi.

Każda Organizacja powinna przeprowadzić analizę ryzyka w obszarze ataków DDoS na swoją infrastrukturę teleinformatyczną i na podstawie wyników tej analizy dobrać odpowiednie narzędzia (w tym z poniższej listy), rozwiązania techniczne, czy optymalny model architektury dostępowej do Internetu w celu ochrony przed atakami typu odmowa usługi.

II. Metody przeciwdziałania atakom DDoS

Poniższy katalog nie jest zamknięty, może stanowić natomiast wskazówkę jakie komponenty warto wziąć pod uwagę wzmacniając odporność infrastruktury Organizacji na ataki, czy wykonując analizę ryzyka, aby ocenić przygotowanie Organizacji w poszczególnych obszarach.

1. Aktywne zarządzanie routingiem

Po stronie Organizacji łącze do Internetu powinno być zorganizowane poprzez dedykowany węzeł dostępu do Internetu z wykorzystaniem protokołu BGP z ustaloną (tj. zdefiniowaną i opisaną w dedykowanym dokumencie) polityką peeringową/polityką wymiany ruchu IP ze światem zewnętrznym.

Umożliwia to i dokumentuje świadomy dobór tras routingowych w zależności od lokalnej mapy Internetu. Dla każdej Organizacji trasy do Internetu wyglądają nieco inaczej i konieczne jest świadome podejmowanie decyzji o sposobie wymiany ruchu m.in. poprzez wykorzystywanie natywnych mechanizmów protokołu BGP takich jak:

a) dla ruchu wychodzącego *local pref* oraz *community*;
b) dla ruchu przychodzącego *prepend* i *community*. W przypadku redundantnych łączy do tego samego operatora możliwość sterowania ruchem przychodzącym za pomocą metryk *MED,* z możliwością propagacji prefiksów z maską dłuższą niż /24 celem rozłożenia ruchu pomiędzy redundantne urządzenia po stronie Organizacji.

Jednak najważniejszym sposobem wyboru tras jest właściwy dobór operatorów telekomunikacyjnych i peeringów lokalnego otoczenia, w szczególności w międzyoperatorskich węzłach wymiany ruchu.

Należy stosować także klucze MD5 na sesjach BGP pomiędzy Organizacją a operatorami telekomunikacyjnymi co znacząco ogranicza ryzyko ataków (np. BGP hijacking) lub błędu konfiguracyjnego.

Zastosowanie RPKI ROA dla przestrzeni adresowej organizacji dodatkowo ochroni Organizację przed próbami przejęcia tras routingu. Kluczowe jest także utrzymanie aktualnych zapisów w bazie RIPE-DB. Zalecane jest również rozważenie mechanizmów automatyzujących aktualizację bazy RIPE-DB.

Warto rozważyć także zastosowanie filtrów w konfiguracji BGP w celu ograniczenia ryzyka wstrzyknięcia niepoprawnych tras do routingu.

Jednocześnie w celu minimalizacji ryzyk związanych z obszarem routingu zalecamy zapoznanie się z zestawem dobrych praktyk opisanych jako „*Mutually Agreed Norms for Routing Security*”[6].

[6] Źródło: https://www.manrs.org/

2. Struktura połączenia z siecią Internet

Właściwie opracowana i zaimplementowana architektura zapewniająca dostęp Organizacji do sieci Internet jest najistotniejszym elementem wzmacniającym odporność na ataki typu odmowa usługi. Podłączenie organizacji do sieci w odpowiedni sposób zapewnia (obok obniżenia kosztów operacyjnych czy drastycznej poprawy parametrów pracy serwisów i usług Organizacji dla użytkowników zewnętrznych i wewnętrznych) zarówno znaczące zwiększenie odporności infrastruktury sieciowej na ataki, jak i mechanizmy reakcji w przypadku wystąpienia zagrożeń przekraczających pojemność i możliwości przyjęcia ruchu przez zastosowany zestaw łączy.

Dla zapewnienia wyższej odporności przed atakami typu DDoS należy przede wszystkim doprowadzić do sytuacji zwielokrotnienia łączy pomiędzy Organizacją, a siecią Internet. Dywersyfikacja powinna zapewniać zarówno zwyczajną redundancję technologiczną (więcej niż jedno fizyczne połączenie), jak i redundancję wprowadzającą dywersyfikację z uwagi na sam podmiot dostarczający usługi. Zapewnia to nie tylko ochronę przed awariami technologicznymi, ale także przed masowymi awariami w sieci operatora telekomunikacyjnego, problemami natury finansowej czy biznesowej. Organizacja zatem powinna posiadać łącza dostarczane przez więcej niż jednego operatora telekomunikacyjnego, w dodatku w miarę możliwości nie powiązanego ze sobą kapitałowo czy technologicznie.

Warto rozważyć także poddanie ocenie samą jakość usług operatora, oceniając takie parametry jak: przepustowość szkieletu sieci operatora, ilość abonentów końcowych, ilość ruchu w sieci, przepustowość czy wielkość zapasu na łączach międzyoperatorskich i międzynarodowych, rodzaj i jakość stosowanych mechanizmów bezpieczeństwa, podejście operatora do zagadnień cyberbezpieczeństwa, czy wreszcie występowanie nowoczesnych rozwiązań technologicznych w sieci operatora, takich jak wymienione w dalszej części Opracowania *scrubbing center* czy CDN.

Węzeł dostępu do Internetu musi uwzględniać istnienie różnych rodzajów łączy, we właściwy sposób wykorzystując zalety i wady każdego z dostępnych rodzajów. Optymalna konfiguracja dostępu do Internetu obejmować będzie zatem współistnienie łączy różnego typu tak, aby sumarycznie zaspokoić potrzeby Organizacji w zakresie komunikacji – można wyobrazić sobie węzeł, w którym obok zdublowanego łącza międzynarodowego, występują 2-3 łącza od operatorów krajowych oraz podłączenie do dwóch niezależnych węzłów wymiany ruchu międzyoperatorskiego poprzez które dostępne są także sieci CDN. Takie podejście należy uznać za optymalne, zapewniające zarówno najbardziej optymalny model kosztowy, jakość i parametry dla użytkowników końcowych, jak i realną odporność na ataki typu DDoS.

Łącza wykorzystywane przez Organizację jako łącza do Internetu powinny być podzielone na:

a) Łącza do tranzytu ruchu międzynarodowego (tranzyt ogólny);
b) Łącza do tranzytu ruchu krajowego (tranzyt krajowy);
c) Łącza peeringowe dedykowane do ruchu krajowego (peering) i bezpośrednie łącza peeringowe (lokalne peeringi bezpośrednie - jako podklasa łącz peeringowych);
d) Łącza do zasobów (w tym CDN).

	Koszt	Przepustowość	Ilość hopów	Opóźnienia	Ilość użytkowników (dostępność)	Prawdopodobieństwo skutecznego ataku DDoS	Priorytet
Łącze tranzytowe międzynarodowe	Relatywnie wysoki	Ograniczona	B. duża	Duże	Cały Internet	B. duże	4
Łącze tranzytowe krajowe	Relatywnie wysoki	Ograniczona	Średnia	Średnie	Cały kraj	Znikome	3
Łącze peeringowe krajowe	Niski	B. duża	Zerowa	Pomijalne	Ograniczona do uczestników węzłów wymiany ruchu	Znikome	2
Łącze do zasobów	Niski	B. duża	Zerowa	Pomijalne	Brak	Zerowe	1

Tabela 1 – Zestawienie ogólnej charakterystyki łącz dostępowych do Internetu. Źródło: opracowanie własne

Powyższa tabela zawiera podsumowanie cech łączy poszczególnych typów, ze szczególnym zwróceniem uwagi na cechy, przydatne do ich doboru w węzłach dostępu do Internetu w Organizacji.

Poszczególne typy łączy różnią się między innymi takimi parametrami jak:

1) **Koszt** – mierzonym jako ilość złotych za każdy dostępny gigabit przepustowości;
2) **Przepustowość** – mierzoną jako możliwa do uzyskania dla Organizacji przepustowość na łączu danego typu, przy zachowaniu racjonalnych kosztów pozyskania takiego łącza;
3) **Ilość hopów** – rozumiana jako ilość AS dostępnych przez łącze danego typu oraz średnią długość ścieżki (AS-patch) przy dostępie do danego zasobu; łącze jest tym bardziej niezawodne i oferuje lepsze parametry im średnia długość ścieżki do zasobów czy użytkowników jest najkrótsza;
4) **Opóźnienia** – mierzone jako ilość ms typowa pomiędzy Organizacją a użytkownikiem lub zasobem;
5) **Ilość użytkowników** – zasięg danego łącza rozumiany jako ilość i rodzaj zasobów dostępnych poprzez łącze danego typu;
6) **Prawdopodobieństwo ataku DDoS** – rozumiane jako prawdopodobieństwo, że na łączu danego typu pojawi się skuteczny atak, o wolumenie realnie zagrażającym organizacji;
7) **Priorytet** – rozumiany jako zalecaną kolejność routowania, jeśli dany zasób jest dostępny więcej niż jedną trasą – im niższa wartość, tym łącze powinno być bardziej preferowane.

Rodzaje łączy to:

a) Łącze tranzytowe międzynarodowe

Służy do komunikacji ze wszystkimi użytkownikami i usługami dostępnymi w Internecie. Łącza te charakteryzują się relatywnie wysokimi kosztami za 1 gigabit pasma oraz ograniczoną przepustowością (w rozumieniu maksymalnej prędkości pojedynczej sesji TCP). Średnia długość ścieżki BGP i ścieżki traceroute jest największa, co wpływa negatywnie na niezawodność (potencjalne awarie węzłów pośredniczących multiplikowana przez ilość węzłów) oraz opóźnienia (wnoszone przez węzły pośredniczące). Na tym łączu zwykle występują duże opóźnienia liczone w ms. To łącze może przejąć w całości ruch z dowolnego innego rodzaju łącza opisanego

w tabeli (tzw. backup ostatniej szansy). W związku z charakterystyką tego łącza jest ono najbardziej narażone na prawdopodobieństwo skutecznego ataku DDoS o charakterze wolumetrycznym.

Łącze to powinno być wykorzystywane do komunikacji ze światem zewnętrznym jako łącze o najniższym priorytecie – do obsługi ruchu który nie pojawia się na innych rodzajach łącz, głównie ruchu z zagranicy oraz jako backup ostatniej szansy.

W przypadku ataków DDoS o skrajnej wielkości czasowe wyłączenie tranzytu międzynarodowego przywraca dostępność usług dla klientów krajowych i może być traktowane jako ostatni punkt procedury reakcji na masywny atak DDoS.

b) Łącze tranzytowe krajowe

Służy do komunikacji ze wszystkimi użytkownikami polskiego Internetu. Łącze tego typu charakteryzuje się relatywnie wysokim kosztem za 1 gigabit pasma oraz nieco większą przepustowością niż łącza tranzytowe międzynarodowe. Na łączach tranzytowych krajowych występują stosunkowe krótkie ścieżki BGP i traceroute (nie więcej niż kilka węzłów pośredniczących), co pozytywnie wpływa na niezawodność i jakość transmisji tego łącza. Na łączu tego typu występują średnie opóźnienia liczone w pojedynczych milisekundach. Ze względu na charakterystykę tego łącza tj. dostarczanie do Organizacji ruchu od polskich użytkowników Internetu, jest ono w znikomym stopniu narażone na ataki DDoS, ze względu na znacząco ograniczoną ilość użytkowników polskiego Internetu w stosunku do Internetu światowego oraz znaną lokalizację użytkowników (ograniczoną geograficznie do obszaru PL). Ilość hostów będących potencjalnie częściami dowolnych sieci botnet, które mogą zostać wykorzystane do ataków DDoS przez to łącze jest w znikoma w stosunku do ilości hostów zlokalizowanych w Internecie światowym co znacząco zmniejsza prawdopodobieństwo i skalę takiego ataku.

Ruch na tym łączu jest kluczowy do obsługi polskich użytkowników Internetu – ponad 90% ruchu może przechodzić tym łączem (chyba że użytkownik jest dostępny przez łącze peeringowe – informacja poniżej).

W praktyce oznacza to, że odcięcie wszystkich innych łączy telekomunikacyjnych (z powodu awarii lub skutecznego ataku DDoS na łącze tranzytowe międzynarodowe) nie zaburzy w istotny sposób funkcjonowania usług świadczonych przez Organizację dla użytkowników na terenie Polski.

Kluczową cechą tego rodzaju łącza, jest także fakt, że służby państwowe poprzez współpracę z operatorami telekomunikacyjnymi są w stanie w każdym przypadku dotrzeć do użytkownika końcowego generującego ruch (co zapewnia brak anonimowości i pełną atrybucję).

Łącze to powinno być wykorzystywane do komunikacji z użytkownikami krajowymi, o ile użytkownicy ci nie są dostępni na łączu peeringowym.

c) Łącze peeringowe (IX)

Służy do komunikacji z wybranymi użytkownikami krajowymi, podłączonymi do sieci korzystających z tego samego węzła wymiany ruchu. Jest to łącze o najniższym koszcie za 1 gigabit, przy jednoczesnej największej przepustowości, a zatem najlepszej jakości dotarcia do użytkowników.

Na łączu peeringowym zazwyczaj sieć z której korzysta użytkownik końcowy (klient) dostępna jest w dokładnie jednym węźle pośredniczącym którym jest węzeł wymiany ruchu. Skutkuje to najniższymi opóźnieniami w stosunku do łącz tranzytowych krajowych i zagranicznych. Ilość użytkowników dostępnych przez to łącze stanowi podzbiór tranzytowego łącza krajowego – nie wszyscy użytkownicy krajowi dostępni są przez łącza IX (ale ci którzy są dostępni przez te łącza dostępni są przez nie z dużo lepszą jakością). Łącza peeringowe stanowią zatem uzupełnienie krajowego łącza tranzytowego znacząco obniżając koszt i poprawiającą jakość usług komunikacji użytkownika z Organizacją. Łącza peeringowe są często (w zależności od operatora telekomunikacyjnego) dostępne za darmo lub za niewielką opłatą jako rozszerzenie tranzytowego łącza krajowego. Często wykorzystują one ten sam fizyczny interfejs i niewykorzystane pasmo tranzytowego łącza krajowego. Podobnie jak w przypadku łącza tranzytowego krajowego, prawdopodobieństwo oraz skuteczność wystąpienia ataku DDoS jest znikome. Organizacja w swojej polityce peeringowej może określić sposób wymiany ruchu z uczestnikami węzła wymiany ruchu z dokładnością do pojedynczego AS[7] co pozwala w sytuacji kryzysowej (np. ataku DDoS pochodzącego od klienta/klientów z konkretnego AS) na rekonfigurację routingu tj. przełączenie ruchu z tego AS np. na łącze tranzytowe krajowe lub łącze tranzytowe międzynarodowe (co znacząco może obniżyć wolumen złośliwego ruchu) lub w skrajnym przypadku odcięcie danego AS. Dodatkowo podobnie jak w przypadku łącza tranzytowego krajowego, użytkownicy końcowi łącza są znani operatorowi telekomunikacyjnemu wymieniającego ruch w ramach węzła peeringowego. Służby państwowe poprzez współpracę z operatorami telekomunikacyjni są w stanie dotrzeć w każdym przypadku do użytkownika końcowego generującego ruch (brak anonimowości / pełna atrybucja). Ponadto długość tras BGP przez węzły międzyoperatorskie jest najkrótsza, co w znacznym stopniu ogranicza ryzyko ataku typu BGP hijacking.
Przeniesienie części ruchu krajowego na łącza peeringowe spowoduje nie tylko poprawę komunikacji z użytkownikami dostępnymi przez te łącza, ale także poprawę komunikacji z pozostałymi użytkownikami poprzez zmniejszenie ilości ruchu na łączach tranzytowych krajowych i łączach tranzytowych międzynarodowych.

d) Łącza do zasobów (CDN)

Łącza tego typu wykorzystywane są do komunikacji z zasobami, które muszą charakteryzować się wysoką przepustowością i krótkim czasem odpowiedzi. Oznacza to zasoby lub usługi, które muszą być zlokalizowane maksymalnie blisko użytkownika i być w stanie dostarczyć treści szybko i wysokiej jakości. Przykładem takich zasobów są serwisy chmurowe (np. o365, GSuite), portale społecznościowe i usługi streamingowe generujące z natury dużo ruchu. Łącza do zasobów obsługują pojedyncze wybrane usługi lub zasoby, ale ze skrajnie wysoką jakością dostosowaną do

[7] Autonomous System

charakterystyki tych usług. Zastosowanie łącz dostępowych pozwala istotnie poprawić parametry odczuwalne przez użytkownika, równocześnie zdejmując z pozostałych łącz (tj. tranzytowych łącz międzynarodowych, krajowych oraz peeringowych) znaczną część ruchu. Bezpośrednie łącze do CDN zapewnia działanie usług tam zlokalizowanych nawet w przypadku masywnego ataku DDoS na pozostałe łącza wykorzystywane przez Organizację.

Łącza do zasobów dostępne są u operatorów telekomunikacyjnego w ramach:

- Dedykowanego VC/VLAN (analogicznie jak łącze peeringowe) do węzła wymiany ruchu w ramach istniejącej usługi np. jako kolejny kanał istniejącego łącza,
- Usług CDN dostępnych zwykle w węzłach wymiany ruchu międzyoperatorskiego (łączach peeringowych),
- Poprzez bezpośrednie wstawienie urządzeń od dostawcy usługi (np. Google, Youtube, Netflix, Facebook, AKAMAI, CloudFalre itd.) do sieci odbiorcy. W sytuacji, w której odbiorca spełnia wymagania/kryteria dostawcy usługi, urządzenia wstawione do sieci odbiorcy (w domyśle Organizacji) jest bezpłatne lub dostępne w relatywnie niskiej cenie. Zaletą tego rozwiązania jest znaczące odciążenie ruchu na pozostałych łączach, poprzez przeniesienie dostępu do zawartości usług dostawcy (np. Google) do cache zlokalizowanego w sieci Organizacji, co znacząco wpływa na podniesienie jakości usług dostawcy.

Łącze do zasobów to łącze o relatywnie niskim koszcie przepustowości danych per 1 gigabit. Na tego typu łączu, zasoby dostawców usług dostępne są bezpośrednio z wykorzystaniem jednego węzła pośredniczącego w wymianie ruchu. W związku z powyższym opóźnienia transmisji danych na tym łączu są najmniejsze ze wszystkich wskazanych łącz. Na łączach do zasobów nie występuje ruch generowany przez użytkowników końcowych, jednak zastosowanie tego łącza może znacząco odciążyć pozostałe łącza wykorzystywane przez Organizację poprzez przeniesienie ruchu generowanego przez Organizację do dostawców usług np. do serwisu Google. Na łączu CDN nie występuje ryzyko ataku DDoS. Jeżeli zasoby dostawcy usługi dostępne są poprzez takie łącze powinien być to priorytetowy wybór trasy do tego zasobu.

3. CDN

Optymalną metodą dotarcia do użytkowników końcowych z usługami i treściami udostępnianymi przez Organizację jest zastosowanie mechanizmów CDN (*Content Delivery Network*). Rozwiązania tego typu działają jako cache lub proxy zlokalizowane sieciowo bardzo blisko infrastruktury klienta końcowego. Operatorzy telekomunikacyjni często stosują takie rozwiązania w celu poprawy jakości dostępu do typowego kontentu (np. Youtube, Netflix, Google) oraz odciążenie szkieletu sieci i łączy tranzytowych. Szacuje się, że 60% ruchu w Internecie zamyka się obecnie w sieciach CDN i nie jest tranzytowana natywnie do dostawców usług. W praktyce wydajność sieci CDN wielokrotnie przekracza dostępne obecnie wolumeny największych ataków DDoS, co wydaje się wystarczającym zabezpieczeniem przed atakami.

Usługi CDN mogą być dostarczane na trzy sposoby:

1) Jako usługa CDN dostarczana przez dużego, międzynarodowego dostawcę, świadczącego usługi CDN dla dowolnej zawartości;

2) Jako usługa dostępna u operatora telekomunikacyjnego, dostarczającego dowolną zawartość bezpośrednio do użytkowników zewnętrznych z węzłów CDN, zamiast z serwerów Organizacji;
3) Jako usługa dużych podmiotów, którzy wstawiają swoje urządzenia typu cache do sieci obsługującej odpowiednio duży ruchu kliencki. Takie rozwiązania stosuje np. Google, czy Netflix.

Organizacja powinna rozważyć zastosowanie CDN jako metody dotarcia do użytkowników końcowych, jeśli kontent pozwala na tego typu pośrednika. Przy wyborze CDN jako metody dostarczania zawartości Organizacja musi wziąć pod uwagę zasięg geograficzny sieci CDN oraz lokalizację swoich użytkowników (nie ma żadnego sensu udostępnianie usług dostępnych typowo dla rynku polskiego poprzez międzynarodowych graczy CDN na cały świat). Organizacja powinna uwzględnić także rekomendacje i regulacje prawne związane z chmurowym udostępnianiem usług i ich lokalizacją na terenie UE (przepisy RODO, regulacje KNF).

4. Nadmiarowe pasmo

Przy małych atakach wolumetrycznych często wystarczającym zabezpieczeniem może być posiadanie nadmiarowego pasma w odniesieniu do konkretnego łącza telekomunikacyjnego. Podczas produkcyjnego użytkowania łącza lub infrastruktury/systemów teleinformatycznych suma użytkowanego pasma nie powinna przekraczać 50% dostępnych zasobów (rozumianych jako dostępne pasmo na danym linku). W celu ochrony przed tego typu atakami możliwe jest wykupienie od operatora telekomunikacyjnego usługi 95 (lub 98) percentyl. Jest to usługa polegająca na posiadaniu dużo szerszego pasma ruchu niż zakontraktowane z opłatą za ruch po przekroczeniu danego kontraktu. Przykładowo jeżeli wolumen ruchu przekroczy zakontraktowane pasmo to operator telekomunikacyjny automatycznie przydziela klientowi dodatkowe pasmo (płatne zazwyczaj w modelu ilość gigabitów x ilość godzin przydzielenia dodatkowego pasma).

5. Bitrate łącza

Ważnym parametrem zapewniającym jakość i dostępność usług jest bitrate łącza (rozumiany jako ilość bitów jaką można przesłać w jednostce czasu) po stronie dostawcy danej usługi, czyli Organizacji. Większy bitrate uzyskujemy poprzez zastosowanie szybszych (nadmiarowych w stosunku do prędkości łącza po stronie Organizacji) interfejsów sieciowych (min. 10 Gbit/s ze względu na konstrukcję tego typu interfejsu tj. głębokość kolejek FIFO, moc obliczeniowa układów użytych do obsługi danego interfejsu) oraz poprzez zwielokrotnienie ilości samych interfejsów. Ma to na celu skrócenie czasu obsługi pakietów danych przez urządzenia sieciowe i odciążenie kolejek FIFO na tych urządzeniach. Należy mieć na względzie prędkości łączy dostępnych u użytkowników końcowych, które w związku z efektem skali mogą mieć znaczenie w przypadku generowaniu połączeń użytkowników do infrastruktury teleinformatycznej Organizacji.

W chwili obecnej operatorzy telekomunikacyjni dostarczają klientom indywidualnym łącza nierzadko o bitrate przekraczającym 1Gbit/s. W związku z czym należy zapewnić świadczenie usług Organizacji łączem o parametrach nie gorszych niż łącza wykorzystywane przez klientów. Zapobiega to kolejkowaniu pakietów po stronie Organizacji, a zatem odciąża urządzenia i infrastrukturę Organizacji, poprawiając zarówno

responsywność technologiczną serwisów/usług Organizacji (odczuwalną dla użytkowników końcowych), jak i odporność na przeciążania i ataki.

Należy przy tym pamiętać, że także operator telekomunikacyjny w swojej sieci szkieletowej i dostępowej musi mieć dostępne nadmiarowe pasmo, które powinno zapewniać poprawną pracę sieci operatora w przypadku typowego ataku DDoS. Upewnienie się co do posiadanego przez operatora pasma (zarówno w szkielecie, jak i do podłączenia węzła terminującego usługi Organizacji) może być elementem analizy poprzedzającej zakup łącza.

6. Blackholing

W przypadku wystąpienia wolumetrycznego ataku DDoS, zarówno dostawca łącza internetowego, jak i Organizacja mają możliwość zablokowania ruchu przychodzącego poprzez skierowanie go do tzw. *black hole* tj. do nieistniejącego interfejsu *(/dev/null*).

Blackholing może być realizowany na dwa sposoby:

a) Poprzez dopisanie odpowiednich reguł kierujących złośliwy ruch do blackhole przez dostawcę usługi (ręcznie lub automatycznie);
b) jako usługa udostępniona klientowi (Organizacji) przez operatora telekomunikacyjnego do samodzielnej realizacji w zakresie udostępnionych łącz telekomunikacyjnych.

W porównaniu do metody polegającej na filtrowaniu ruchu, rozwiązanie to charakteryzuje się dużo mniejszym zużyciem zasobów routerów, jak i prostszym zarządzaniem regułami niż stosowanie klasycznych list ACL. Daje to możliwość skutecznego i szybkiego zablokowania niepożądanego ruchu przy minimalnej konsumpcji zasobów urządzeń.

Zastosowanie blackholingu niesie za sobą ryzyko zablokowania poprawnej adresacji w przypadku np. błędnego wprowadzenia adresów/klas adresów, a w efekcie może mieć wpływ np. na:

a) dostępność usług świadczonych przez Organizację,
b) dostępność usług zewnętrznych dostawców,
c) stabilność sieci w przypadku zablokowania adresacji istotnej z punktu widzenia działania sieci Internet (DNS, RIPE DB, CDN itd.).

Należy mieć na uwadze, że ręczne zastosowanie reguł blackholingowych będzie wymagało również ręcznego usunięcia tych reguł np. w momencie ustania ataku.

Organizacja wybierając dostawcę łącza internetowego powinna weryfikować czy dany dostawca posiada wdrożony w swojej sieci blackholing.

7. BGP flow specification (flowspec)

Flowspec jest mechanizmem stosowanym po stronie operatora telekomunikacyjnego, rozszerzającym protokół BGP o warstwę 4 modelu OSI tj. oprócz routingu opartego o adresację IP umożliwia konfigurację tras routingu w oparciu o usługi oraz wykorzystanie dodatkowych flag pozwalających na skierowanie części ruchu inną trasą, zdefiniowaną przez administratora. Dla przykładu w sytuacji ataku DDoS DNS Amplification przy

wykorzystaniu mechanizmu flowspec istnieje możliwość przekierowania tego ataku (z wykorzystaniem portu 53) np. do usługi cleaning center operatora telekomunikacyjnego, przy jednoczesnym zachowaniu dostępności usług opartych o inne protokoły jak np. HTTPS.

W odróżnieniu od w/w rozwiązania blackholing mechanizm flowspec pozwala operatorowi telekomunikacyjnemu na odfiltrowanie złośliwego ruchu sieciowego kierowanego na dany adres IP Organizacji od ruchu poprawnego, co pozwala na zachowanie działania świadczonych dla klientów usług.

Flowspec może być realizowany na dwa sposoby:

c) Poprzez dopisanie odpowiednich reguł kierujących złośliwy ruch do flowspec przez dostawcę usługi (ręcznie lub automatycznie),
d) jako usługa udostępniona klientowi (Organizacji) przez operatora telekomunikacyjnego do samodzielnej realizacji w zakresie udostępnionych łącz telekomunikacyjnych (możliwe jest zestawienie sesji BGP FS, gdzie Organizacja sama zarządza regułami przekazywanymi do operatora telekomunikacyjnego).

Zastosowanie mechanizmu flowspec niesie za sobą ryzyko zablokowania poprawnych usług lub adresacji w przypadku np. błędnego wprowadzenia adresów/klas adresów/portów/usług, a w efekcie może mieć wpływ np. na:
a) dostępność usług świadczonych przez Organizację,
b) dostępność usług zewnętrznych dostawców wykorzystywanych przez Organizację,
c) stabilność sieci w przypadku zablokowania adresacji istotnej z punktu widzenia działania sieci Internet (DNS, RIPE DB, CDN itd.).

Przy wyborze operatora telekomunikacyjnego Organizacja powinna rozważyć obligatoryjne wykorzystanie mechanizmu flowspec przez tego operatora.

8. Usługi cleaning center

Usługi cleaning center świadczone przez operatorów telekomunikacyjnych polegają na istnieniu w sieci operatora urządzeń umożliwiających odfiltrowanie ruchu złośliwego od ruchu poprawnego. Cleaning center zapewnia znacznie wyższą skuteczność filtrowania niepożądanego ruchu sieciowego od rozwiązań blackhole oraz flowspec.

W sytuacji wykrycia ataku, operator telekomunikacyjny przekierowuje atak (z wykorzystaniem np. Flowspec lub podstawowego BGP) do dedykowanej usługi. Administrator usługi wykorzystując zaawansowane algorytmy odfiltrowuje niepożądany ruch sieciowy zidentyfikowany jako atak. Pozostały ruch sieciowy kierowany jest do sieci Organizacji.

Ważną cechą takich rozwiązań, jest praca w trybie off-ramp, co oznacza że w normalnej sytuacji ruch produkcyjny nie jest w ogóle kierowany do takiego cleaning center. Powoduje to brak opóźnień, skraca ścieżkę przejścia pakietu, oraz minimalizują ryzyko awarii (awaria cleaning center nie powoduje niedostępności usługi podstawowej). Zwiększa to także istotnie pojemność takiego cleaning center odciążając go od ruchu, który nie wymaga filtrowania.

Operator telekomunikacyjny powinien zapewnić wysoką dostępność usług cleaning center np. poprzez:

a) redundancję,
b) rozproszenie geograficzne.

Jako jedno z ryzyk wykorzystania usługi cleaning center można wskazać potencjalne błędy false positive polegające na błędnym wyfiltrowaniu poprawnego ruchu produkcyjnego. Zastosowanie rozwiązań inline (opisanych poniżej) współpracujących z rozwiązaniami po stronie operatora telekomunikacyjnego pozwala dodatkowo na znaczne skrócenie czasu detekcji ataku i odfiltrowanie niepożądanego ruchu sieciowego.

9. Rozwiązania chmurowe

Dostępne na rynku rozwiązania chmurowe należy traktować jako usługę cleaning center on demand, gdzie w przypadku ataku DDoS najkorzystniejszą trasą w ścieżce BGP będzie trasa przez cleaning center podmiotu świadczącego taką usługę Organizacji.
Podstawową wadą takiego rozwiązania jest fakt, że całość ruchu Organizacji w tym ruch klientów może zostać przekierowana poprzez odległy węzeł na świecie, co całkowicie zaburza lokalną politykę routingu, w istotny sposób pogarsza parametry usługi dla klientów oraz powoduje wątpliwości prawne w zakresie możliwości przetwarzania czy analizy ruchu użytkowników przez podmiot znajdujący się w ścieżce takiej komunikacji.
Zastosowanie tego typu rozwiązań powinno być zawsze zweryfikowane pod kątem zgodności z rekomendacjami i przepisami prawa obowiązującymi w danym sektorze. Dokonana ocena musi w szczególności uwzględniać sposób w jaki cleaning center analizuje ruch oraz czy dochodzi do przetwarzania danych transmitowanych w ramach zabezpieczonych w ten sposób usług.

10. Rozwiązana inline

Oprócz usług i rozwiązań chroniących Organizację przed atakami DDoS, które są realizowane przez operatorów telekomunikacyjnych, Organizacja powinna posiadać własne elementy infrastruktury teleinformatycznej pozwalające na ochronę przed atakami DDoS.
Pozwala to na:

a) wczesne wykrycie ataków tego typu i niezwłoczne powiadomienie operatora telekomunikacyjnego,
b) mitygację ataku (do pojemności łącza Organizacji) poprzez odfiltrowanie złośliwego ruchu od ruchu poprawnego,
c) nałożenie limitów ruchu sieciowego do pojemności łącza Organizacji lub pojemności zasobów infrastruktury Organizacji, co pozwala na ochronę przed atakiem DDoS ukierunkowanym na wysycenie zasobów infrastruktury lub aplikacji,
d) ochronę przed wykorzystaniem infrastruktury Organizacji do generowania ataków DDoS na inne instytucje/Organizacje (np. z wykorzystaniem DNS Amplification).

Zastosowanie rozwiązania inline, jako jedynej metody ochrony przed atakami typu DDoS, nie może być rozważana jako skuteczna mitygacja tego typu zagrożeń.

Należy zwrócić uwagę, że zastosowanie rozwiązań inline stanowi jedyną realną opcję odparcia ataków DDoS ukierunkowanych na logikę aplikacji bez przekazywania kluczy szyfrujących poza Organizację (ruch jest deszyfrowany przez samą Organizację).

11. Filtrowanie ruchu sieciowego

Zgodnie z zasadami minimalizacji uprawnień niezbędnych do świadczenia danej usługi Organizacja powinna rozważyć filtrowanie ruchu sieciowego wyłącznie do ruchu niezbędnego do działania danej usługi.

Rozwiązanie to pozwoli na ograniczenie potencjalnego złośliwego ruchu sieciowego docierającego do urządzeń świadczących usługę, a nie związanego z tą usługą. Ma to zastosowanie zarówno w odniesieniu do warstwy aplikacyjnej jak i sieciowej. Dla przykładu jeżeli świadczoną usługą jest np. dostęp poprzez protokół HTTPS to pozostały ruch sieciowy kierowany do innych usług tego urządzenia (świadczącego usługę HTTPS) powinien być filtrowany (ograniczony). Podobnie w przypadku świadczenia usługi poprzez protokół TCP, ruch sieciowy UDP, ICMP itd. kierowany do tego urządzenia powinien być filtrowany (ograniczony).

Jako ryzyko w/w rozwiązania można przyjąć niedoszacowanie mocy urządzeń sieciowych filtrujących ruch, co w efekcie może powodować przeciążenie urządzenia oraz brak realizacji podstawowych jego funkcji, w tym ograniczenie dostępu do usług świadczonych przez Organizację.

12. Control-plane policing

Wykorzystując mechanizmy dostępne na danych urządzeniach należy wdrożyć polityki regulujące przepływ ruchu kontrolnego dla usług realizowanych przez dane urządzenie. Przykładowo jeżeli router Organizacji świadczy usługi dostępu do Internetu z wykorzystaniem protokołu BGP, należy wdrożyć odpowiednie, zgodnie z rekomendacjami producenta, mechanizmy filtrowania i limitowania zasobów urządzenia tak, aby komunikaty kontrolne protokołu BGP przetwarzane były tylko od zweryfikowanych sąsiadów.

13. Właściwe wymiarowanie sprzętowe urządzeń sieciowych

W atakach DDoS ukierunkowanych na wysycenie zasobów może dochodzić do wysycenia zasobów urządzeń obsługujących połączenia sieciowe (wysycenie pamięci, wysycenie procesora, kolejki FIFO, procesory na kartach liniowych, dedykowane do obsługi dedykowanych funkcji routera procesory FPGA, limity równoległych połączeń dla danej platformy sprzętowej itd.), co w efekcie może prowadzić do niedostępności usług sieciowych.
Organizacja powinna zapewnić właściwe wymiarowanie urządzeń sieciowych wykorzystywanych do transmisji danych. Parametry urządzenia powinny być dobrane w taki sposób, aby zapewnić możliwość obsługi ruchu o co najmniej rząd wielkości większego niż typowy ruch produkcyjny w Organizacji.

14. Load balancing oraz proxowanie ruchu sieciowego

Organizacja powinna rozważyć wdrożenie architektury, w której serwisy i usługi Organizacji są chronione poprzez dodatkową warstwę dostępową wystawioną dla klienta z Internetu. Warstwa ta powinna zapewniać odpowiednie reguły bezpieczeństwa pozwalające na inspekcję ruchu sesji klienta. Istnienie warstwy pośredniej tzw. proxy pomiędzy Internetem a warstwą front end w Organizacji pozwoli na zabezpieczenie infrastruktury Organizacji przed wysyceniem zasobów na serwerach aplikacyjnych świadczących usługi.

Warstwa proxy powinna zostać wykorzystana również do filtrowania ruchu sieciowego z punktu widzenia ochrony warstwy aplikacyjnej poprzez zastosowanie rozwiązań klasy WAF/DAF.

Odpowiednia konfiguracja parametrów warstwy proxy (limity sesji, TLS offloading, one-connect, connection persistance, itd.) pozwali zoptymalizować wykorzystanie zasobów na serwerach aplikacyjnych i pozwali ograniczyć negatywne skutki ataków, które mogą w istotny sposób wpłynąć na stabilność i bezpieczeństwo systemów warstwy back-end.

15. Captcha

Organizacja powinna rozważyć zastosowanie mechanizmów ochrony przed atakami DDoS na warstwę aplikacyjną poprzez wymuszenie faktycznej interakcji z użytkownikiem poprzez zastosowanie rozwiązań takich jak:

a) Captcha ze szczególnym uwzględnieniem UX,
b) mechanizmów pozwalających na ograniczenie ruchu generowanego automatycznie przez klienta,
c) wykrycia działań botów lub aplikacji automatycznie generujących ruch do usług świadczonych przez Organizację.

Rozwiązanie takie chroni również przed atakami typu brute force.

Przy doborze rozwiązania należy zwrócić uwagę na fakt, że darmowe rozwiązania Captcha dostępne na rynku mogą zbierać metadane użytkowników oraz przekierowywać ruch użytkowników do dostawcy rozwiązania Capcha co powoduje, że faktyczny koszt korzystania z darmowych rozwiązań uiszczany jest poprzez zapłatę metadanymi użytkownika końcowego, co z kolei może stanowić naruszenie przepisów prawa.

16. DNS

Organizacja powinna rozważyć wdrożenie rozwiązań technicznych i organizacyjnych zabezpieczających przed atakami DDoS ukierunkowanymi na niedostępność usług DNS utrzymujących domeny Organizacji. Działanie usługi DNS jest niezbędne do działania usług Organizacji dostępnych dla użytkowników zewnętrznych. Unieruchomienie serwisu DNS organizacji w praktyce oznaczać będzie niedostępność usługi analogicznie do masywnego ataku DDoS.

Główną metodą ochrony przed atakami na DNS jest wdrożenie architektury rozproszonej serwisu DNS – bardzo trudno jest wykonać atak DDoS, który zablokuje jednocześnie dużą liczbę serwerów DNS, rozporoszonych geograficznie. Dostępne są na rynku usługi oferujące rozproszenie secondary DNS na kilkaset rozsianych po świecie miejsc, z możliwością wskazania lokalizacji geograficznej takich serwerów, co w praktyce zdaje się wyczerpywać zarówno wymogi techniczne związane z bezpieczeństwem, jak i wymogi prawne związane z przetwarzaniem danych na terenie UE.

III. Procedury

Organizacja powinna posiadać stosowne procedury realizowane w sytuacji wystąpienia ataków DDoS, w tym m.in.:

a) procedury kontaktu z operatorami telekomunikacyjnymi, określające szybkie ścieżki eskalacji na wypadek identyfikacji ataku DDoS,
b) procedury dot. priorytetyzacji usług Organizacji, które w sytuacji wystąpienia ataków DDoS umożliwią zarządzanie tymi usługami (np. ograniczenie dostępności usług o mniejszym priorytecie, zapewniając działanie usług o wyższym priorytecie). W celu optymalizacji oraz przyspieszenia realizacji procedur w tym obszarze Organizacja powinna rozważyć ich automatyzację,
c) procedury dot. komunikacji kryzysowej (uwzględniające komunikację z użytkownikami, przedstawicielami mediów, organem nadzoru, organami państwa, dostawcami zewnętrznymi itd.) realizowane w sytuacji skutecznego ataku DDoS, ograniczającego dostępność usług Organizacji,
d) procedury identyfikujące kluczowe osoby niezbędne do podjęcia działań w sytuacji ataku oraz umożliwiające im podjęcie tych działań (np. wskazujące na konieczność stawienia się w biurze Organizacji w sytuacji niedostępności usług, definiujące decyzyjność itd.),
e) procedury dot. komunikacji z właściwym zespołem CSIRT (sektorowym lub poziomu krajowego) w celu niezwłocznego powiadomienia o zidentyfikowanym ataku.

IV. Testy

Organizacja powinna określić a następnie realizować harmonogram regularnych i cyklicznych testów:

a) odporności infrastruktury na ataki DDoS w celu określenia parametrów granicznych tej odporności,
b) testowania procedur wewnętrznych.

Każdorazowo po zakończeniu testów lub w przypadku wystąpienia realnego ataku DDoS, Organizacja powinna przeprowadzić ponowną analizę ryzyka uwzględniającą co najmniej:

- konieczność aktualizacji procedur,
- konieczność aktualizacja architektury teleinformatycznej, w tym architektury podłączenia do sieci Internet,
- aktualizację urządzeń w obszarze właściwego wymiarowania ich zasobów.

V. Monitoring bezpieczeństwa

W związku z powszechną dostępnością działań cyberprzestępczych w formule CaaS (*cybercrime as a service*) również przeprowadzenie ataku DDoS wiąże się ze stosunkowo niskim kosztem po stronie atakującego.
Ataki DDoS mogą być wykorzystane do odwrócenia uwagi od innych ataków i działań przestępczych prowadzonych w tym samym czasie w stosunku do innych usług i serwisów Organizacji.
W sytuacji wykrycia ataku DDoS Organizacja powinna zapewnić monitorowanie bezpieczeństwa infrastruktury i usług w stopniu nie gorszym niż przy standardowym ruchu użytkowników i bezawaryjnym świadczeniu usług.

VI. Zarządzanie WAN out of band

Organizacja powinna zapewnić możliwości zarządzania swoją infrastrukturą teleinformatyczną (np. zarządzanie siecią WAN) w przypadku ataku DDoS, poprzez zapewnienie alternatywnych (zapasowych, nadmiarowych) łącz wykorzystywanych dla celów administracyjnych, które powinny być odrębne od pasma wykorzystywanego do świadczenia usług Organizacji.

W sieciach telekomunikacyjnych tworzonych w obrębie Organizacji zgodnie z najlepszymi praktykami powinna powstać dedykowana infrastruktura umożliwiająca dostęp do konsoli zarządzania co najmniej do kluczowych komponentów tejże infrastruktury. Jak pokazują przypadki *case study*[8], całkowita separacja od infrastruktury produkcyjnej zapewni niezakłócony dostęp do konsoli zarządzającej urządzeń w przypadku rozległych awarii bądź trwającego rozległego ataku. Większość nowoczesnych urządzeń sieciowych wyposażona jest w dedykowane interfejsy przeznaczone do zarządzania tymi urządzeniami, które to interfejsy są wyposażone we własne dedykowane procesory i układy sieciowe. Oznacza to, że nawet w przypadku rozległego ataku DDoS powodującego wysycenie zasobów sprzętowych urządzeń sieciowych lub serwerów, administratorzy będą mieli nadal zagwarantowane dedykowane zasoby sprzętowe, aby obsługiwać konsolę tego urządzenia w celu podjęcia działań mitygujących.

VII. Rozdzielenie ruchu korporacyjnego od usług dla użytkowników zewnętrznych

Rozdzielenie ruchu dedykowanego aplikacjom i usługom świadczonym użytkownikom zewnętrznym od ruchu pochodzącego z biur, oddziałów Organizacji lub pracowników Organizacji pracujących zdalnie, pozwoli na zbudowanie niezawodnej sieci, w której zasoby sprzętowe oraz dostępne łącza będą dedykowane do konkretnych zadań. Pozwoli to także zapewnić odpowiednie mechanizmy kontroli, filtrowania i ochronę, które mogą różnić się pomiędzy wymaganiami centrów przetwarzania danych, a użytkownikami zlokalizowanymi w oddziałach Organizacji, w tym także użytkownikami mobilnymi Organizacji.
Infrastruktura dedykowana ruchowi aplikacyjnemu/usługom świadczonym użytkownikom zewnętrznym może mieć o wiele większe zapasy „mocy" w stosunku do infrastruktury biurowej wykorzystywanej przez pracowników Organizacji, w tym przede wszystkim Organizacja może

[8] Źródło: https://datacenterfrontier.com/facebook-we-disconnected-our-data-centers-from-the-internet/

wykorzystać dostępne usługi bezpieczeństwa i scrubbingu danych, aby na poziomie operatora telekomunikacyjnego odpowiednio łagodzić negatywne skutki ataku DDoS.

Pracownicy biurowi Organizacji jak i pracujący zdalnie mogą łączyć się z wewnętrznymi systemami Organizacji zarówno za pomocą łącz internetowych, jak i za pomocą dedykowanych transmisji danych pomiędzy placówkami Organizacji, a centrami przetwarzania danych.
Organizacja powinna rozważyć dostępność zapasowego koncentratora VPN dla kluczowych pracowników Organizacji umożliwiający realizację zadań w sytuacji awaryjnej. Organizacja powinna również opracować procedury awaryjne na wypadek niedostępności połączeń VPN obejmujące swoim zakresem konieczność fizycznej obecności pracowników w Organizacji.
W przypadku wykorzystywania przez Organizację usług zewnętrznych dostawców należy rozważyć zastąpienia komunikacji z tymi dostawcami poprzez sieć Internet, łączami dedykowanymi np. w technologii IP MPLS.

VIII. Automatyzacja realizacji scenariuszy awaryjnych

Organizacja powinna dążyć do wprowadzenia zautomatyzowanych mechanizmów, które zadziałają w sytuacji awaryjnej. Są to np. scenariusze, które w przypadku wykrycia ataku mogącego zagrozić ciągłości pracy Organizacji pozwoliłyby na natychmiastowe wdrożenie ustalonych z góry mechanizmów ochrony i łagodzenia skutków potencjalnego ataku. Automatyczne uruchomienie pewnych procesów takich jak np. zmiana atrybutów prefiksu rozgłaszanego w BGP, wdrożenie dodatkowych mechanizmów ochrony zasobów sprzętowych urządzeń sieciowych i serwerów (*control-plane policing),* czy w skrajnych przypadkach wyłączenie łącza internetowego, które jest przedmiotem ataku w znacznym stopniu może przyczynić się skrócenia czasu reakcji Organizacji na atak. W długiej perspektywie takie podejście ograniczać będzie negatywne skutki ataku dając administratorom czas na odpowiednią atrybucję oraz wdrożenie szczegółowych dedykowanych mechanizmów ochronnych. Realizacja tego scenariusza wymaga jednak wdrożenia infrastruktury out-of-band management oraz przygotowania i przetestowania stosownych scenariuszy oraz umieszczenia ich w planach BCP. Należy mieć również na uwadze ryzyka związane z automatyzacją procesów, które w przypadku błędnej implementacji mogą w skrajnym przypadku doprowadzić do niedostępności usług Organizacji.

IX. Podsumowanie

Nie istnieją gotowe, kompleksowe rozwiązania ani jedna uniwersalna metoda ochrony przed atakami typu DDoS. Budowanie infrastruktury odpornej na ataki nie może być sprowadzone wyłącznie do kupienia gotowego produktu czy usługi, lecz powinno być systemowym podejściem do zaprojektowania całego łańcucha technologicznego odpowiedzialnego za dostarczenie ostatecznej usługi, tworząc wielowarstwową ochronę Organizacji zgodnie z zasadą *defence in depth.*
Faktyczna, wypadkowa odporność organizacji na atak jest sumą zastosowanych rozwiązań i technik przeciwdziałania z wykorzystaniem maksymalnej dostępnej dla Organizacji liczby opisanych powyżej rozwiązań i technik oraz uwzględnieniem potencjalnego wpływu najsłabszego ogniwa.

Znaczenie kolorów TLP dla odbiorców wiadomości

TLP: RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.
TLP: AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane.
TLP: GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP: WHITE	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).