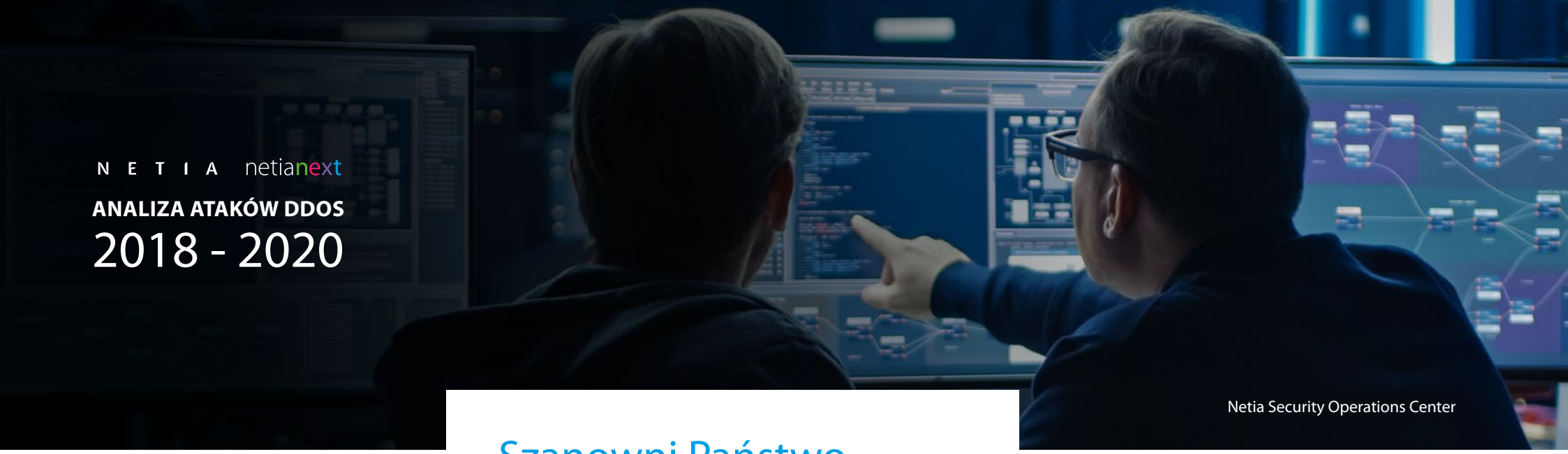
NETIA netianext

ANALIZA ATAKÓW DDOS

2018 - 2020



NETIA netianext

ANALIZA ATAKÓW DDOS

2018 - 2020

Netia Security Operations Center

Szanowni Państwo

Oddajemy w Państwa ręce podsumowanie pracy specjalistów **Działu Nadzoru Sieci i Security Operations Center Netii** z ostatnich trzech lat (2018-2020) w obszarze ochrony naszej sieci, a tym samym Klientów biznesowych Netii. Przyjrzeliśmy się dokładniej atakom **DoS i DDoS**, które od lat sieją spustoszenie wśród użytkowników sieci na całym świecie. Jako dostawca usług teleinformatycznych, w tym wielu rozwiązań Cyberbezpieczeństwa, chronimy między innymi przed atakami DDoS ponad 300 Klientów.

Analizując szczegółowo dane z platformy, która w Netii „obserwuje" ruch sieciowy, zebraliśmy je w formie zagregowanych i zanonimizowanych wniosków, które pozwoliły nam na identyfikację pewnych trendów i zachowań w działaniach cyberprzestępców. W poniższej publikacji skupiliśmy się na wybranych, najbardziej ciekawych wnioskach, które są jednocześnie ważne dla naszych Klientów, bowiem wpływają na ciągłość działania ich biznesu.

Co więcej? Przybliżymy Państwu skalę problemu, potencjalne konsekwencje dla Użytkowników, a także jakie wymagania (w tym również regulacyjne) są stawiane obecnie przed biznesem w sferze Cyberbezpieczeństwa. Odpowiemy też na dość przewrotne pytanie – czy można stać się atakującym nie wiedząc o tym?

Zapraszam do lektury!

Rafał Bakalarz
Dyrektor Sprzedaży B2B ds. ICT

CZYM JEST DDoS?

Na czym polegają ataki DDoS i co grozi Tobie lub Twojej Firmie, jeśli się nie ochronisz?

Atak **DDoS** (ang. Distributed Denial of Service) inicjowany jest przez wysyłanie wielu zapytań, a tym samym przewymiarowanego ruchu, do konkretnego serwisu (np. sklepu, strony www), systemu (np. systemu rezerwacji, aplikacji biletowej) czy urządzenia (np. routera brzegowego, serwera danych), co prowadzi do przekroczenia dostępnej przepustowości i zasobów. W efekcie, Twoi klienci nie mają dostępu do Twoich usług przez Internet, a w skrajnych sytuacjach, elementy infrastruktury IT, jak serwery, czy routery brzegowe, mogą ulec awarii lub zniszczeniu.

Jak to się dzieje?

Zapytania przychodzą z wielu rozproszonych (Distrubuted) zainfekowanych maszyn (tzw. "zombies"), które połączone w jedną sieć (tzw. "botnet") wysycają przepustowość jaką jest w stanie obsłużyć łącze i infrastruktura. To prowadzi do paraliżu danego serwisu.

Przykład ataku na **sklep internetowy**

Kto może paść ofiarą?

Szczególnie zagrożone atakami DDoS są usługi i platformy internetowe, gdyż cyberprzestępcy atakują usługi o kluczowym znaczeniu dla firmy, "zalewając" sieć fikcyjnym ruchem.

Ataki DDoS są często skierowane przeciwko dużym firmom oraz bankom. Takie działania mogą być przyczyną utraty wiarygodności firmy, jeśli jej użytkownicy nie wiedzą, dlaczego strona internetowa, sklep lub usługa nie działa. Z tych powodów, poznanie sposobów na powstrzymywanie i zapobieganie atakom DDoS jest kluczowe dla działania wielu firm. W ostatnich latach notujemy znaczny wzrost ataków na firmy średnie oraz małe, ale nierzadko zdarzają się też ataki na użytkowników prywatnych.

Jak działają cyberprzestępcy i **jakie narzędzia** do tego wykorzystują?

Atak DDoS z założenia **ma wywołać paraliż.**

Co gorsze, nie jest trudny do przeprowadzenia.

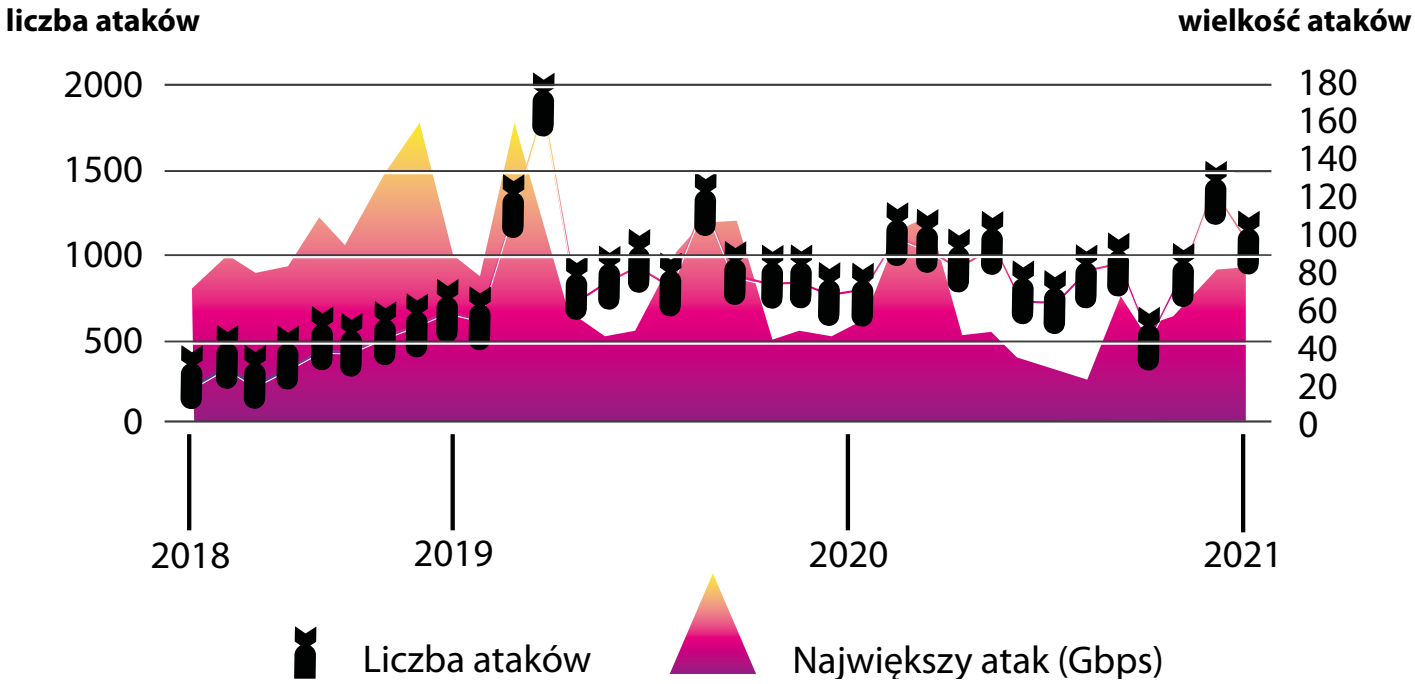
O ile zdobycie setek czy tysięcy zainfekowanych urządzeń (nie tylko komputerów osobistych, ale i np. urządzeń IoT) i połączenie ich w gotową do ataku armię (tzw. sieć botnet) nie jest prostym zadaniem, o tyle już wynajęcie takiego botnetu w ramach usługi - dużo łatwiejsze (skalę zwielokrotni dostępność technologii 5G i liczba podpiętych urządzeń). Czarnorynkowe ceny zaczynają się od kilku dolarów za godzinę. Cena rośnie wraz z wolumenem ataku (w Gbps) oraz poziomem ochrony potencjalnej ofiary. Przeliczając to na polskie warunki, przykładowy sklep internetowy można sparaliżować na długie godziny nie wydając na to nawet tysiąca złotych.

Wielu naszych Klientów prowadzi komercyjne serwisy, a ataki na nich identyfikujemy najczęściej w okresach wzmożonych zakupów, np. przed świętami Bożego Narodzenia lub Walentynkami.

Z przeprowadzonej analizy wynika, iż mamy wielu Klientów atakowanych regularnie i bardzo intensywnie. Liczby ataków w przypadku pojedynczych firm nierzadko przekraczają tysiące! Czas trwania ataku w średniej wielkości firmie wynosi ok. 40 minut, a maksymalnie może sięgać nawet **34 000 minut** (rzeczywista maksymalna wartość u Klienta z sektora publicznego).

W Netii jesteśmy w stanie ochronić takie firmy czy instytucje, dzięki czemu nie odczują paraliżu. Bez aktywnej ochrony mogłyby zniknąć z cyfrowej mapy świata na długie okresy - rekordziści byliby w **tzw. „timeout" nawet do 1 roku!**

Jakub Sawicki
Kierownik Produktów Security



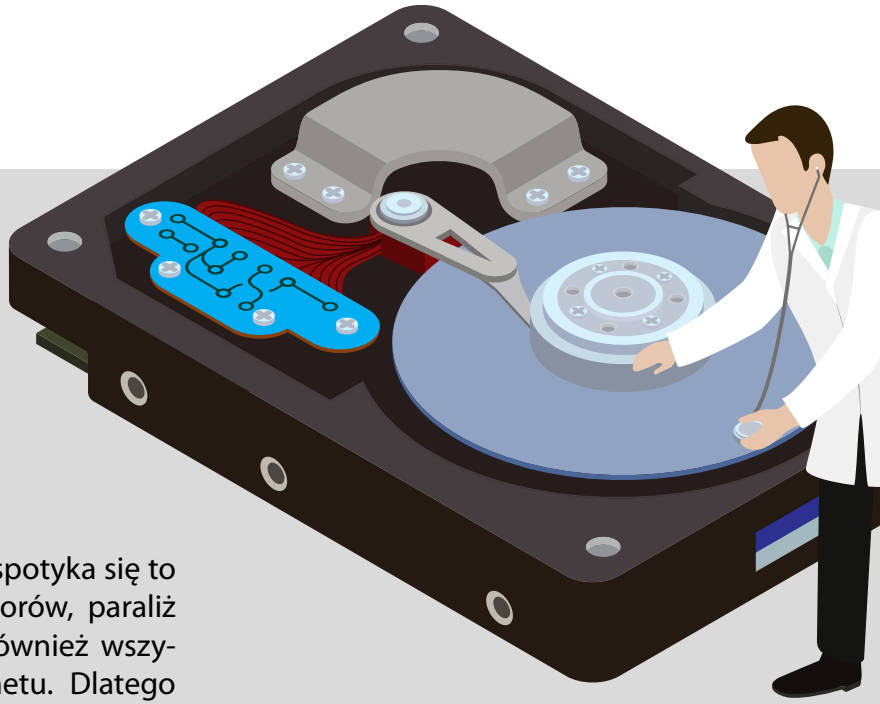
Jakie są konsekwencje?

Tutaj scenariuszy jest wiele. Od chwilowego przestoju w pracy, po żmudne i wielomiesięczne odbudowywanie całego biznesu od nowa.

Jako przykład mogą posłużyć przypadki przeanalizowane w naszej sieci. Klienci objęci ochroną Netia DDoS Protection nie znaleźli się w poniższej analizie przypadków, ponieważ skutecznie osłaniamy ich przed takimi zagrożeniami.

Mały nie znaczy bezbolesny

Ważnym parametrem ataku jest jego wolumen, czyli Mbps, a nawet Gbps. Największe ataki sięgają kilkuset Gbps, a w historii mieliśmy przypadki przekraczające 2 Tbps! Nie oznacza to jednak, że mniejsze ataki można bagatelizować. Nasze doświadczenie wskazuje, że infrastruktura wielu firm nie jest w stanie poradzić sobie z atakiem dotykającym 20-30% ruchu łącza, które mają teoretycznie do wykorzystania. Oznacza to, że dla łącza np. 100 Mbps, nawet atak 50 Mbps (teoretycznie niekrytyczny) może okazać się zabójczy.

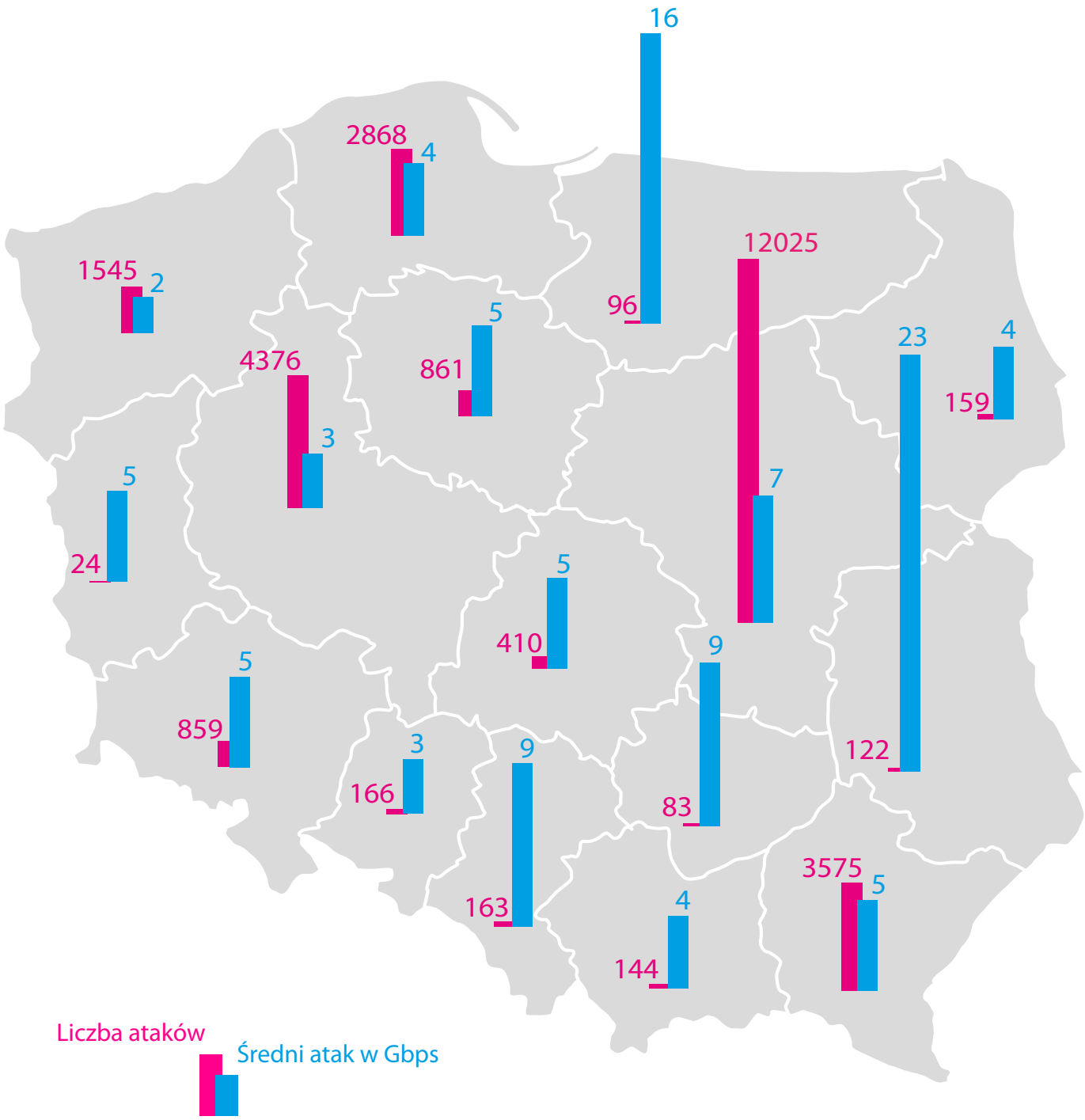


Obawiaj się nie tylko o firmę. Twoje dane też mogą ucierpieć.

Wiele ataków odnotowujemy również na użytkowników prywatnych. W raportach wewnętrznych widnieje to jako atak na ich lokalnego operatora, ale problem ma poważniejsze konsekwencje niż brak Internetu u atakowanego "Kowalskiego". Jeżeli operator nie dba o prawidłową mitygację ataku, czyli skuteczne odpieranie ataków, a spotyka się to niestety często u mniejszych operatorów, paraliż przeżywa nie tylko atakowany, ale również wszyscy klienci danego dostawcy Internetu. Dlatego powszechna staje się opinia o niskiej jakości sieci lokalnego operatora, czego powodem może być nawet jeden użytkownik końcowy.

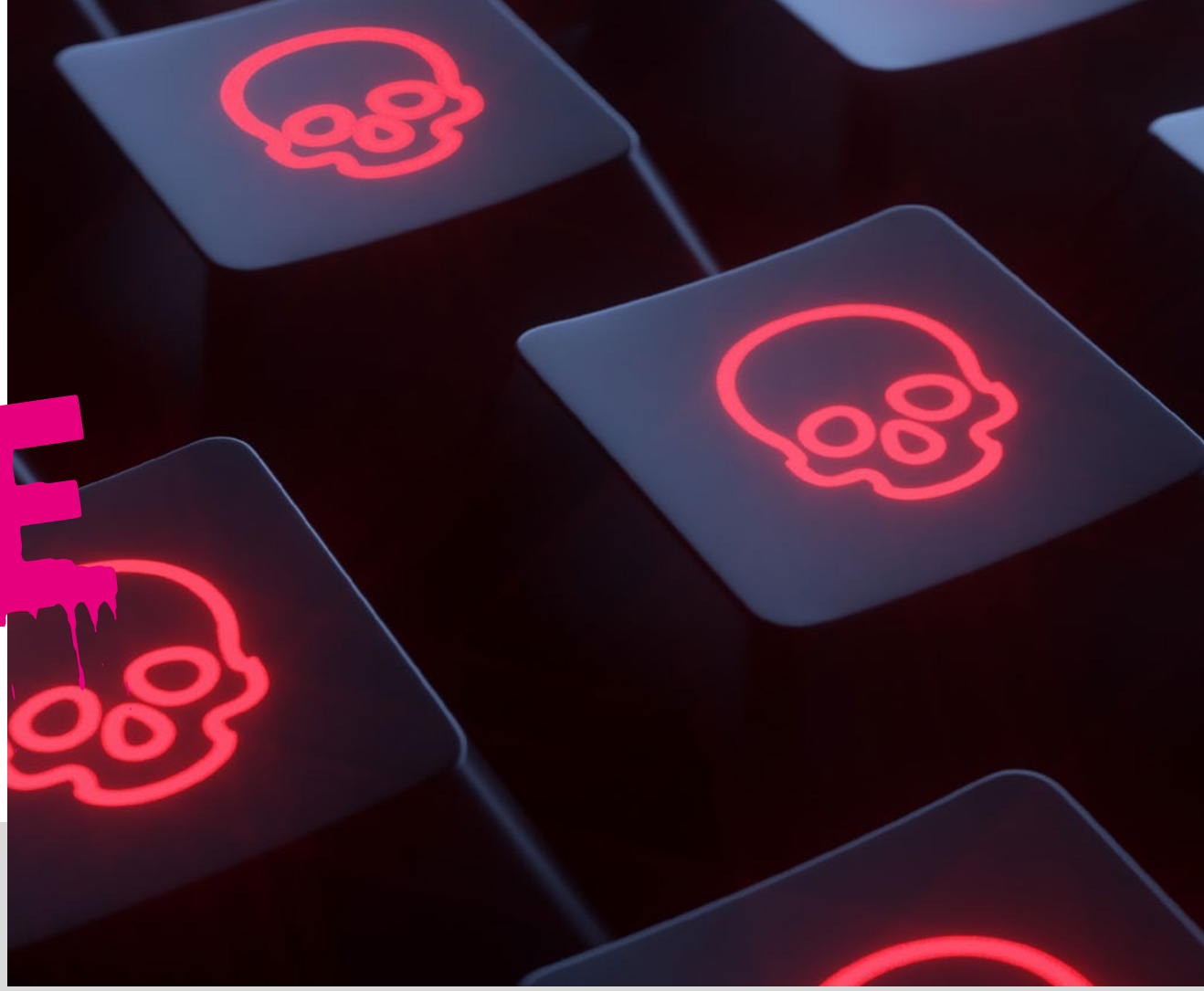
Liczba ataków przypadająca na dane województwo oraz średnia wartość ataku (w Gbps)

Najczęściej atakowanymi są firmy z województwa mazowieckiego, a głównie z Warszawy ze względu na duże zagęszczenie firm i instytucji w tym rejonie. Liczba ta sięga ponad 12 tys. ataków w okresie ponad 2 lat i tutaj też pojawiły się najdłuższe ataki – nawet 24 godziny! Najrzadziej atakowane są firmy z województwa lubuskiego – tylko 24 ataki. Zadziwiające jest to, że średni wolumen ataku nie jest najwyższy w województwie mazowieckim. Ponad, trzykrotnie wyższy jest średni atak w województwie lubelskim oraz dwukrotnie – w województwie warmińsko-lubuskim. Patrząc na wielkość firm, które były tutaj najczęściej atakowane, można wyciągnąć wniosek, że mieliśmy do czynienia z rzadziej prowadzonymi, ale dużo większymi atakami.



SCENARIUSZ 1

ATAK ZOMBIE



Atakujący przy użyciu zainfekowanych komputerów "zombie" skutecznie wysyca pojemność łącza, powodując paraliż działania serwisu. Jest to bardzo popularny sposób działania wśród cyberprzestępców, a jednocześnie najprostszy do przeprowadzenia. Jakie konsekwencje niesie to dla ofiary? Poza brakiem możliwości działania (brak obustronnego kontaktu ze światem) są to straty wizerunkowe.

Przykładowy sklep internetowy, który nie działa, operator lokalny, który notuje przerwy w dostarczanych usługach lub nawet firma prowadząca jedynie stronę internetową - wszyscy tracą zaufanie klientów. Z każdą minutą spada ich operacyjność, liczba klientów, a tym samym tracą pieniądze.

SCENARIUSZ 2

Zasłona dymna

DDoS jako "zasłona dymna". Cyberprzestępcy często łączą wektory ataku. DDoS jest w tym przykładzie wstępem do czegoś "większego" lub zasłoną dymną. Atakowana jest np. platforma chroniąca aplikację firmy lub nawet router brzegowy, który strzeże dostępu do infrastruktury i strategicznych danych.

Cyberprzestępca wysycając pojemność platformy wykorzystuje moment, w którym biznes nie jest chroniony.

Dość powszechny jest tzw. "bypass", który w przypadku awarii przekierowuje automatycznie ruch "obok" platformy chroniącej. Tak stwarza się idealna okazja dla cyberprzestępcy.

SCENARIUSZ 3

ŻĄDANIE $OKUPU

DDoS jako atak dodatkowy. W ostatnich latach bardzo częste są tzw. ataki ransomware (od ang. „ransom" - okup), które wykorzystując złośliwe oprogramowanie, szyfrują wszystkie dane na wszystkich komputerach firmy, co powoduje kompletny paraliż działania. Jaka jest pierwsza reakcja osób odpowiedzialnych za działanie firmy? Odzyskujemy backup! W tym momencie cyberprzestępca dokłada paraliż połączenia atakiem DDoS.

Firma nie tylko traci dane lokalne (zostały zaszyfrowane lub usunięte), ale również nie ma możliwości odzyskania backupu.

Co zatem pozostaje? Negocjować z "terrorystami"? Zapłacić okup? Czekać aż odpuszczą? Nie wszystko stracone – nawet w takim momencie uaktywniona ochrona DDoS Protection pomoże uzyskać połączenie ze światem, a backup (jeśli nie jest zainfekowany) odzyska dane i przywróci działanie organizacji.

Jak przeprowadzić atak DDoS i nie mieć takiej świadomości?

Analiza największych ataków jednoznacznie wskazuje, że napastnicy, żeby zwiększyć swoją skuteczność, wykorzystują kilka technik jednocześnie np. **IP Fragmentation, Total Traffic, UDP, DNS Amplification**. Zestawienie obok przedstawia typy nadużyć najczęściej wykorzystywanych przez przestępców.

Liczby, charakteryzujące poszczególne rodzaje ataków, w ujęciu miesięcznym (grudzień 2020r.) są skategoryzowane według ich „dotkliwości" (tzw. severity).

Paweł Szymkowicz
Kierownik Zespołu Wsparcia ICT

Historia najczęściej zaczyna się w ten sam sposób tj. od kliknięcia przez ofiarę w niesprawdzonego linka, a następnie pobrania i zainstalowania, przez nieświadomego użytkownika, złośliwego oprogramowania. Skutkiem tego jest skryte przejęcie pełnej kontroli nad urządzeniem ofiary. Zaatakowana maszyna, potocznie nazywana "zombie", automatycznie staje się częścią botnetu i może być wykorzystywana z powodzeniem do dokonywania szeregu dalszych przestępstw.

Największe botnety to nawet dziesiątki milionów zainfekowanych maszyn zombie, które mogą być wykorzystywane bez wiedzy i zgody ich właścicieli do przeprowadzania ataków DDoS. Tak rozproszone systemy służą nie tylko ukryciu rzeczywistego napastnika, ale również mają niebagatelny wpływ na skalę potencjalnego incydentu.

Dodatkowym czynnikiem zwiększającym siłę rażenia ataku (amplification attack) jest specyfika powszechnie używanych w Internecie protokołów sieciowych, w przypadku których stosunkowo niewielkie, odpowiednio spreparowane zapytania wysłane przez zombie (modyfikacja źródłowego IP), skutkują znacznie większymi odpowiedziami, które mogą skutecznie sparaliżować atakowany serwer.

Najczęściej wykorzystywanymi protokołami do tego są m. in. NTP (Network Time Protocol), DNS (Domain Name System) czy CLDAP (Connectionless Lightweight Directory Access Protocol).

ALERT TYPE	HIGH	MEDIUM	LOW	TOTAL
Total Traffic Host	395	95	946	1436
IP Fragmentation Host	180	48	357	585
CLDAP Amplification Host	148	8	99	255
UDP Host	145	47	75	267
NTP Amplification Host	139	6	6	151
DNS Amplification Host	64	16	11	91
memcached Amplification Host	18	1	38	57
DNS Host	8	0	529	537
ICMP Host	5	1	3	9
DoS Profiled Router Bandwidth	3	13	130	146
DoS Profiled Router TCP	3	8	35	46
DoS Profiled Router ESP	2	0	0	2
TCP SYN Host	1	0	122	123
SNMP Amplification Host	1	0	0	1
TCP RST Host	0	0	88	88
DoS Profiled Router UDP	0	1	17	18
DoS Profiled Router GRE	0	0	5	5
TCP null Host	0	0	1	1
TCP SYN/ACK Amplification Host	0	0	1	1

Od momentu uruchomienia pierwszego Klienta usługi ochrony przed atakami DDoS w sieci Netia minęło ponad 6 lat. W tym czasie, w związku z dynamicznym rozwojem np. platform i urządzeń IoT, których zabezpieczenia często nie istnieją lub są na poziomie podstawowym, zmieniły się zarówno protokoły wykorzystywane w atakach DDoS, ale przede wszystkim poziom obserwowanych ataków.

Dlatego też, Netia aktywnie rozwija i modernizuje wykorzystywaną platformę, zarówno pod kątem funkcjonalnym (wdrożenie i integracja protokołu flowspec, dodanie możliwości ochrony aplikacyjnej), jak i wydajnościowym – zwiększenie poziomu mitygowanego (czyszczonego ruchu) z 10 Gbps do 50 Gbps.

Barłomiej Zaremba
Dyrektor Departamentu Rozwoju
i Zarządzania Siecią

Jak to wygląda po „inżyniersku”?

Warto zwrócić szczególnie uwagę na deklarowane poziomy czyszczonego ruchu. W wielu przypadkach do ochrony przed atakami wykorzystywany jest **blackholing**. Jest to prosta i tania metoda, która pozwala na zablokowanie ruchu do atakowanego adresu. Niestety jej wadą jest to, że oprócz ruchu niepożądanego blokowany jest też ruch, który jest ruchem produkcyjnym. Trochę więcej możliwości pod tym względem oferuje **flowspec**, ale jest to mechanizm, który dobrze sprawdza się jako uzupełnienie ochrony.

Jak działa ochrona w ramach usługi Netia DDoS Protection?

Netia w swojej infrastrukturze wykorzystuje zarówno mechanizmy oferowane przez blackholing jak i flowspec, przy czym usługa nie opiera się głównie na blokowaniu, ale na czyszczeniu ruchu do atakowanego Klienta.

Cały ruch przychodzący do Klienta objętego ochroną jest monitorowany pod kątem anomalii pojawiających się w jego charakterystyce. Po wykryciu przekroczenia odpowiednio przyjętych parametrów, jest przekierowywany do elementu platformy, który służy do oczyszczenia ruchu. W tym urządzeniu ruch niepożądany jest odfiltrowywany od standardowego ruchu przeznaczonego do danego Klienta.

Tylko ruch „oczyszczony" jest odsyłany dalej w kierunku łącza dostępowego Klienta. Mechanizm ten pozwala na skuteczną ochronę łączy Klienta przed wysyceniem, a co za tym idzie, problemami z działaniem i dostępnością usług.

W ramach obserwowanych zdarzeń w sieci Netii widzimy, że problem ataków DDoS nie dotyczy tylko dużych korporacji. Bardzo częstymi przypadkami są ataki np. na aktywnych użytkowników sieciowych platform dla graczy.

W przypadku klientów operatorów lokalnych (service prividerów), atak na takiego jednego abonenta powoduje problemy wszystkich lub przynajmniej tych, którzy korzystają z tych samych urządzeń dostępowych.

Wojciech Bendig
Kierownik Działu IP i Security

Ciekawostka:

Z przeprowadzonych analiz można zaobserwować korelację ataków DDoS z notowaniami kryptowalut – liczba ataków jest odwrotnie proporcjonalna do wartości tej waluty. Jak można wywnioskować – infrastruktura na co dzień wykorzystywana w atakach DDoS, może też służyć innym celom.

Cyber bezpieczeństwo

to temat-rzeka, dowiedz się więcej:

Aktywnie chronimy całą naszą sieć, wszystkie platformy i dostępne serwisy. Dotyczy to również oferty chmurowej.

Wybierając rozwiązania Netii, dołączysz do grona Klientów, którzy mogą skorzystać z całego portfolio usług bezpieczeństwa, w tym ochrony przed najpopularniejszym atakiem, jakim jest DDoS.

Sebastian Paczkowski
Kierownik ds. Klientów Kluczowych
- Rozwiązania Zintegrowane
(Członek ISACA i ISSA Polska)

Regulacje i Wymogi, które nakładają nowe obowiązki

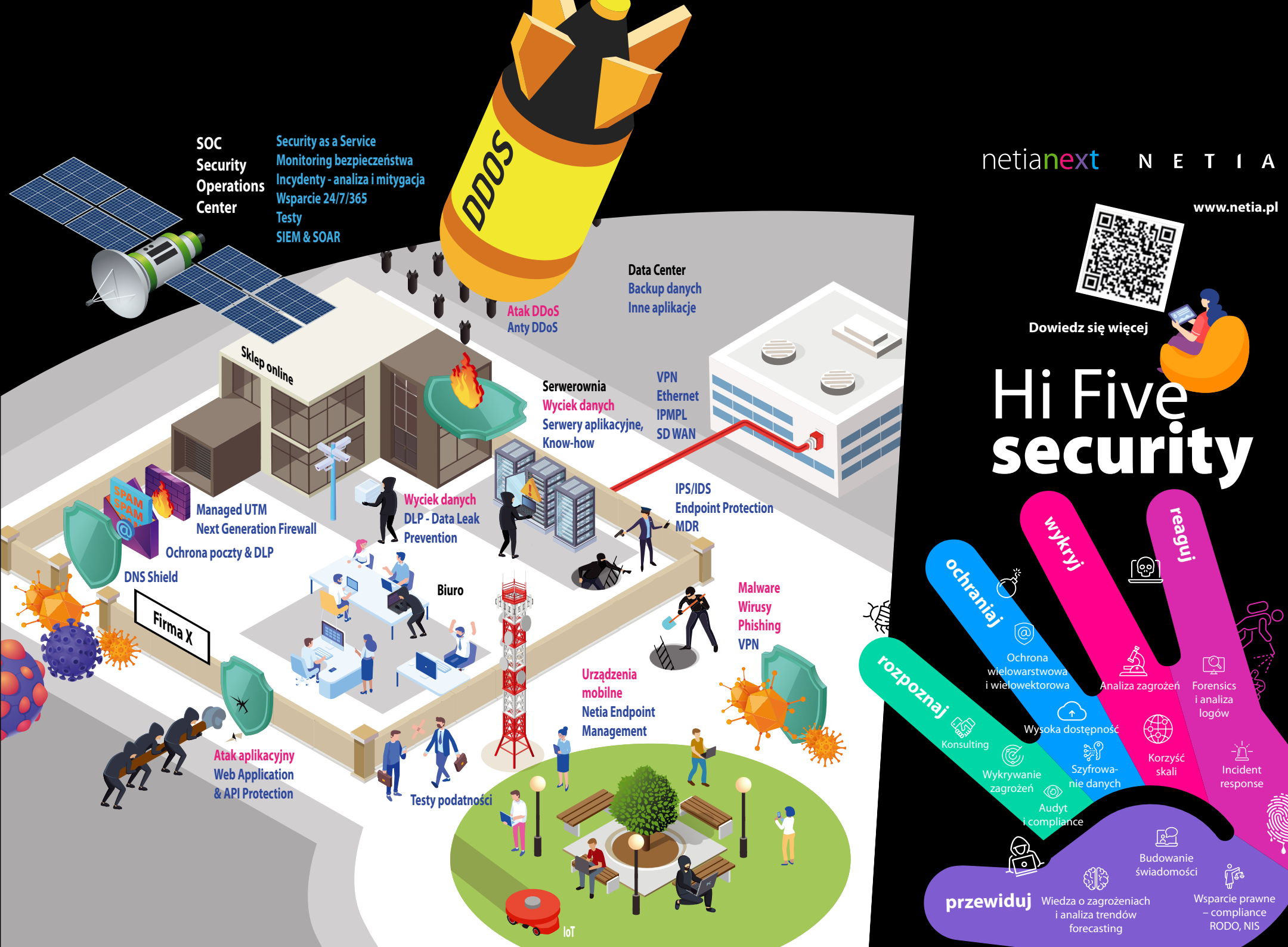
Wiodący operatorzy telekomunikacyjni, świadczący usługi dostępu do Internetu to podmioty, które świadczą usługi kluczowe, określone w ustawie KSC (Krajowy System Cyberbezpieczeństwa), która stanowi implementację dyrektyw NIS i NIS2. Kluczowym aspektem jest infrastruktura krytyczna z punktu widzenia funkcjonowania państwa. Co za tym idzie, podmioty krytyczne powinny posiadać zdolności operacyjne w celu zapobiegania, powstrzymania, reagowania na zagrożenia i incydenty, a także wytworzenia cyberodporności oraz fizycznej odporności własnej sieci i systemów informatycznych.

Niewątpliwie, ataki wolumetryczne DDoS z perspektywy operatora to incydent, który wpływa na dostępność i wydajność największych wartości operatora, czyli sieci i punktów wymiany ruchu z operatorami globalnymi, co ma bezpośrednie przełożenie na dostępność systemów IT, łączności, aplikacji, danych, informacji własnych i Klientów.

Operator, aby chronić siebie i swoich Klientów, monitoruje punkty wymiany ruchu i sieć. Wykorzystuje struktury SOC (Security Operations Center) i NOC (Network Operation Center), aby podejmować działania zapobiegające, wykrywające, a także mitygujące ataki DDoS.

W ramach wytycznych NIS2 operator powinien wdrożyć m. in. mechanizmy:

- analizy ryzyka i polityki bezpieczeństwa systemów informatycznych,
- ciągłości działania,
- zarządzania kryzysowego,
- bezpieczeństwa łańcucha dostaw,
- bezpieczeństwa w pozyskiwaniu, rozwijaniu i utrzymywaniu sieci i systemów informatycznych (w tym obsługa i ujawnianie podatności),
- procedur (testowanie i audyt) służących ocenie skuteczności środków zarządzania ryzykiem Cyberbezpieczeństwa.



netianext NETIA

www.netia.pl

Dowiedz się więcej

Hi Five security

RAPORT Z POLA BITWY

TARGET: NETIA DDOS PROTECTION

TIME: 2018-2020

BATTLEFIELD: POLAND

NETIA netianext

162 Gbps

Największy odparty atak

2587

Najwyższa liczba ataków na jednego klienta

118 KLIENTÓW
miało przynajmniej
10 ATAKÓW

31
miało ponad
100 ATAKÓW!