Raport CERT Orange Polska 2018 w pigułce

ochronę zapewnia
CyberTarcza

sieć #1

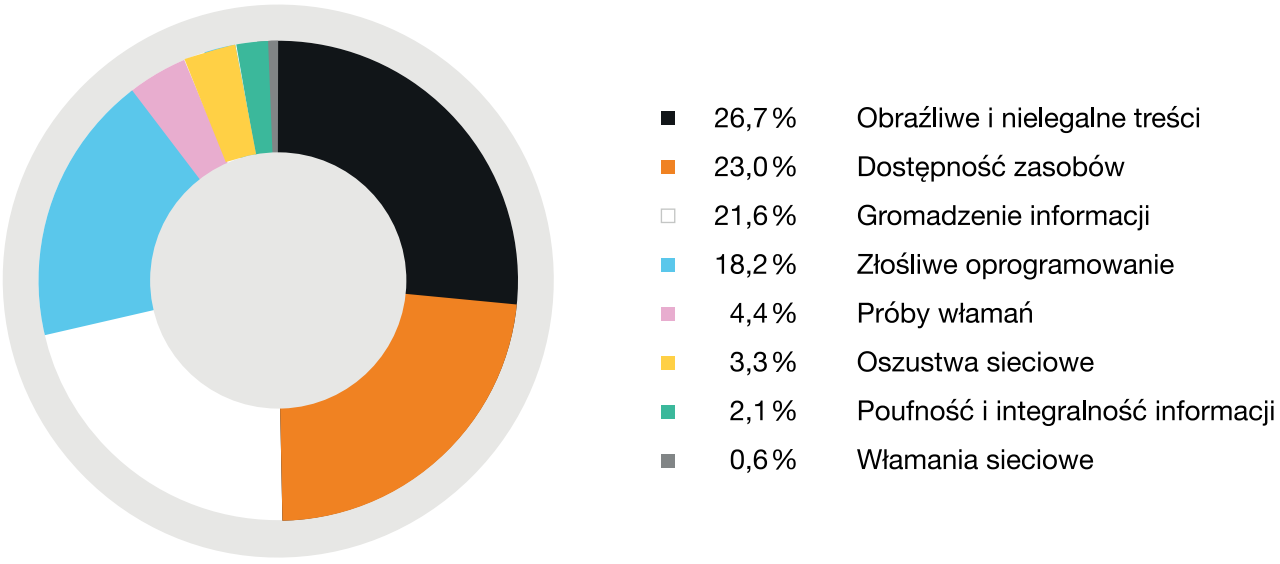
orange™

5 miliardów
– tyle urządzeń internetu rzeczy było podłączonych do sieci, gdy publikowaliśmy pierwszą edycję raportu.
W 2020 roku ta liczba ma wzrosnąć do
20 miliardów.

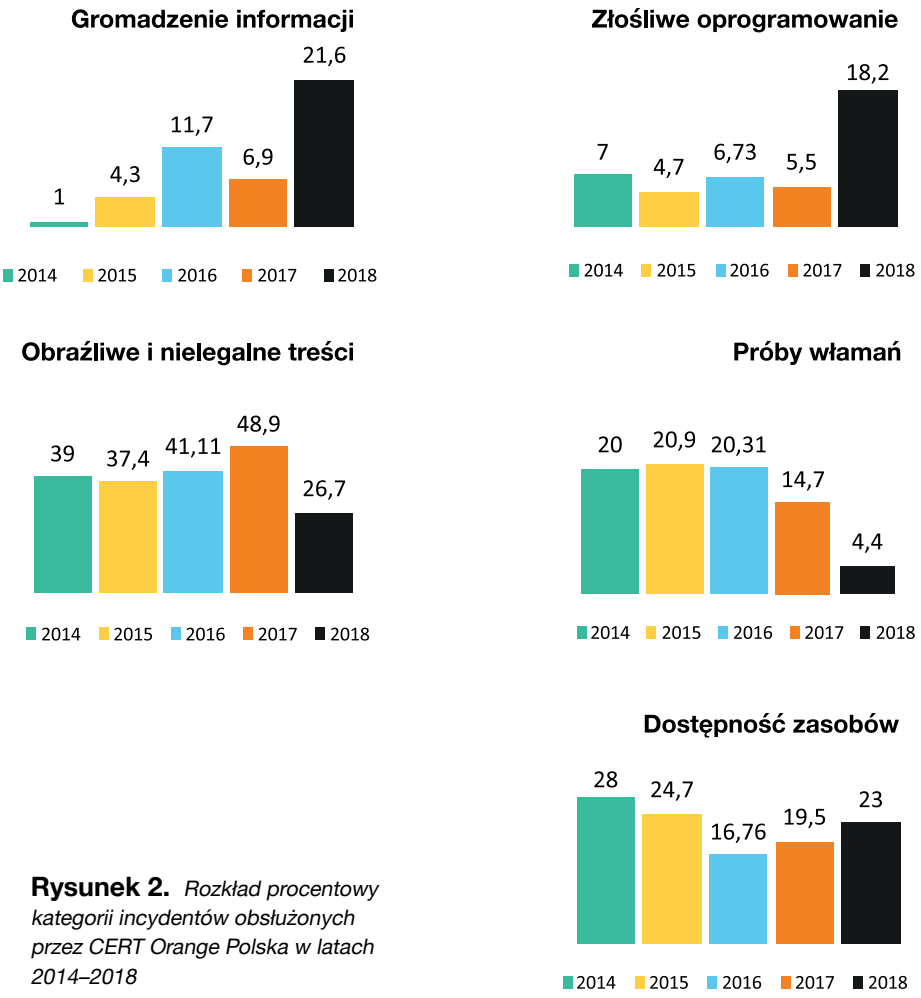
Incydenty bezpieczeństwa obsłużone przez CERT Orange Polska

Wśród obsłużonych incydentów największą grupę (26,7 proc.) stanowiły te z klasy obraźliwych i nielegalnych treści. **W porównaniu z rokiem 2017 nastąpił znaczny spadek - o 22 pp. (48,9 proc. w 2017 r.). Na drugim miejscu znalazły się ataki na dostępność zasobów (23 proc.), podobnie jak w ubiegłym roku (19,5 proc.).** Kolejne miejsca to incydenty z grupy dotyczącej gromadzenia informacji (21,6 proc.) – tutaj odnotowano znaczny wzrost w stosunku do poprzedniego roku (6,9 proc. w 2017 r.); złośliwe oprogramowanie (18,2 proc.) – istotny wzrost w porównaniu z poprzednim rokiem (5,5 proc. w 2017 r.); próby włamań (4,4 proc.) – duży spadek w stosunku do poprzedniego roku (14,7 proc. w 2017 r.), oszustwa sieciowe (3,3 proc.) – podobnie jak w ubiegłym roku (2,9 proc. w 2017 r.). Kategorie incydentów najrzadziej występujących stanowiły ataki na poufność i integralność informacji – 2,1 proc. (0,4 proc. w 2017 r.). Poniżej 1 proc. zaklasyfikowano włamania sieciowe.

Inne, nieobjęte wspomnianymi kategoriami, stanowiły 0,1 proc. incydentów. W 2018 r. rozkład w czasie występowania incydentów nie był regularny. Przede wszystkim można zauważyć znaczny wzrost liczby obsługiwanych incydentów w ostatnim miesiącu roku, czyli w okresie świątecznym – wówczas złośliwe kampanie zbierają największe żniwa. Wykorzystywano m.in. phishing poprzez wysyłanie fałszywych faktur, podszywając się pod różne firmy (w tym pod Orange).



Rysunek 1. Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w 2018 r.



Rysunek 2. *Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w latach 2014–2018*

Średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska sięgnęła poziomu

2,1 Gbps.

Największa odnotowana wartość natężenia ruchu w szczycie ataku

198 Gbps.

Wybrane wydarzenia i zagrożenia w Polsce w 2018 roku

Styczeń

Fałszywe e-maile podszywające się pod Amazon

Zespół CERT Orange Polska zidentyfikował i przeanalizował kampanię phishingową podszywającą się pod sklep Amazon. Eksperci wykazali, że jest to próba wyłudzenia loginu i hasła.

Luty

Phishing podszywający się pod Orange

Użytkownicy internetu otrzymywali fałszywe e-maile podszywające się pod domenę @orange.pl.

Wyciek danych z rządowego serwisu

Jeden z serwisów uruchomionych przez Ministerstwo Finansów umożliwił zapoznanie się z danymi osób, które miały otrzymać zwrot nadpłaconego podatku PIT. Wśród danych można było odnaleźć m.in. PESEL i NIP podatników.

Marzec

Sprawa Thomasa

Po 6 latach aktywności Tomasz T. (pseudonim Thomas, Armaged0n) został aresztowany przez policję. Cyberprzestępca znany jest z dziesiątek cyberataków skierowanych przeciwko polskim internautom. Za pomocą kampanii e-mailowych infekował złośliwym oprogramowaniem stacje robocze Polaków. Podszywał się m.in. pod Allegro, PayPal, DotPay.

Aktywność malware QuantPro w sieci Orange

Zespół CERT Orange Polska odnotował aktywność malware'u QuantPro. Z przeprowadzonej analizy wynikało, że liczba infekcji to ok. 1500 użytkowników. Dokładna analiza tego malwar'u znajduje się na stronie cert.orange.pl.

Maj

„Loterie" Orange

Podczas przeglądania internetu użytkownicy mogli natknąć się na wyskakujące okno lub zakładkę z informacją „Drogi użytkowniku, gratulacje!". Treść wskazywała, że Orange rzekomo rozdaje smartfony Samsung Galaxy. Aby odebrać jeden z nich, należało wypełnić fałszywą ankietę, podając swoje dane, w tym login i hasło.

Orange Polska i NASK gospodarzami prestiżowego spotkania europejskich CERT-ów

24 i 25 maja w siedzibie Orange Polska spotkali się specjaliści ds. cyberbezpieczeństwa z Europy. To jedno z trzech w roku cyklicznych spotkań organizowanych w ramach inicjatywy Trusted Introducer, zrzeszającej czołowe europejskie zespoły reagowania na zagrożenie bezpieczeństwa teleinformatycznego.

Czerwiec

Kampania mailingowa z biletami na Mundial

W czerwcu, tuż przed Mundialem, internauci otrzymywali e-maile z wiadomością o wygranej biletów na mistrzostwa świata. Aby odebrać nagrodę, należało kliknąć link lub otworzyć złośliwy załącznik w formacie .pdf lub .doc. Kolejnym krokiem było uzupełnienie danych kontaktowych i dokonanie niewielkiej opłaty. Internauci wykonujący powyższe polecenia stracili pieniądze i nie otrzymali biletów.

Lipiec

Incydenty z Fake DNS

W lipcu CERT Orange Polska odnotowywał nawet dwa miliony zdarzeń dziennie powiązanych z Fake DNS. Atak polegał na podmianie adresów serwerów DNS w urządzeniach sieciowych bądź bezpośrednio w przeglądarce.

Sierpień

Złośliwe aplikacje w systemie Android

CERT Orange Polska odnotował w sieci mobilnej ruch złośliwego oprogramowania Bankbot.Anubis. Oprogramowanie to podszywało się pod niegroźną aplikację dostępną na urządzeniach z systemem Android, a jej celem było zmuszenie użytkownika do udzielenia jej dodatkowych uprawnień w zakresie ułatwienia dostępu. Umożliwia to kradzież m.in. loginów i haseł do kont w bankach.

Wrzesień

CyberTarcza wykryła ponad 3 tys. infekcji Bitcoin Minera

CyberTarcza Orange odnotowała 3143 infekcje z wykorzystaniem Bitcoin Minera. To oprogramowanie, które stosuje moc obliczeniową komputera do kopania kryptowalut. Użytkownik często jest nieświadomy zainstalowanego na komputerze oprogramowania.

Listopad

Kamera wysyłała SMS-y, modem nabijał rachunki.

Atak dotyczył sprzętu o stałym adresie IP, korzystającego z usługi VPN Static. Wśród przejętych urządzeń były m.in. routery mobilne, przemysłowe, RUT240, modemy. Po przejęciu kontroli nad urządzeniem przestępcy wykorzystywali je do wysyłania SMS-ów na numery zagraniczne, czerpiąc zarobek z terminowania ruchu SMS.

Modemy przesyłające złośliwe SMS-y

CERT Orange Polska zidentyfikował złośliwe SMS-y z informacją o zwrocie nadpłaty, która jest możliwa poprzez kliknięcie przesłanego linku i wypełnienie formularza. Wiadomości te przygotowane były po angielsku i włosku i skierowane do użytkowników w Wielkiej Brytanii i we Włoszech. Wykorzystane do tego były polskie numery z urządzeń wyposażonych w karty SIM.

Z przeprowadzonych przez zespół CERT Orange Polska analiz wynika, że większa część dystrybucji odbywała się za pomocą reklam, nakłaniających użytkownika do pobrania oprogramowania do optymalizacji działania urządzenia lub darmowego i niesamowicie efektywnego antywirusa.

Aktualne trendy cyberzagrożeń

Rok 2018 niewiele zmienił się, jeśli chodzi o dystrybucję kampanii phishingowych. Użytkownicy polskiego internetu wciąż są atakowani poprzez wykorzystanie socjotechniki. Wydawać by się mogło, że po latach nieustających ataków na skrzynki pocztowe lub profile społecznościowe świadomość internautów nie podda się ewidentnym oszustwom. Niestety, choć można zauważyć poprawę sytuacji (widzimy to np. poprzez liczbę zgłoszeń incydentów), to w dalszym ciągu problem istnieje.

Duży potencjał w obronie przed cyberzagrożeniami eksperci dostrzegają w skutecznym wykorzystaniu sztucznej inteligencji (AI). Tego typu mechanizmy mają wspierać detekcję zagrożeń zarówno na poziomie stacji roboczej użytkownika, jak i na poziomie rozwiązań sieciowych czy usług SOC.

Możliwości, jakie niesie sztuczna inteligencja, mogą znacznie przyspieszyć reagowanie na incydenty zaraz po wykryciu złośliwego oprogramowania. Zautomatyzowane identyfikowanie i analiza zagrożeń będzie możliwa dzięki odpowiednim narzędziom wykorzystującym technologie uczenia maszynowego. Takie rozwiązania, wsparte wiedzą specjalistów, wykazują się wysoką skutecznością w odpieraniu serii ataków.

W 2018 roku zaobserwowaliśmy, że nie ma już większego sensu rozdzielanie ruchu sieciowego na stacjonarny i mobilny. Stale podłączamy nasze telefony do różnych sieci Wi-Fi, więc zagrożenia związane z Androidem masowo pojawiają się w ruchu stacjonarnym. Udostępniamy internet „komórkowy" do komputerów PC (czy nawet konsol do gier), coraz częściej korzystamy też z LTE jako podstawowego medium transmisyjnego – zagrożenia typowe dla PC identyfikowane są w ruchu mobile. Podział na sieć stacjonarną i mobilną przestaje zatem mieć uzasadnienie. Bardziej właściwe wydaje się obecnie kategoryzowanie malware ze względu na platformy „uruchomieniowe" – Android, Windows PC, Linux, w niewielkim stopniu iOS i macOS. Obserwując rok 2018, również można zauważyć pewne charakterystyczne trendy. Oprócz malware „właściwego" typu Triada czy Nymaim, znacznie zwiększyła się liczba incydentów związanych ze szkodliwymi reklamami oraz koparkami kryptowalut.

Wolumetryczne ataki na usługi i infrastrukturę – DDoS

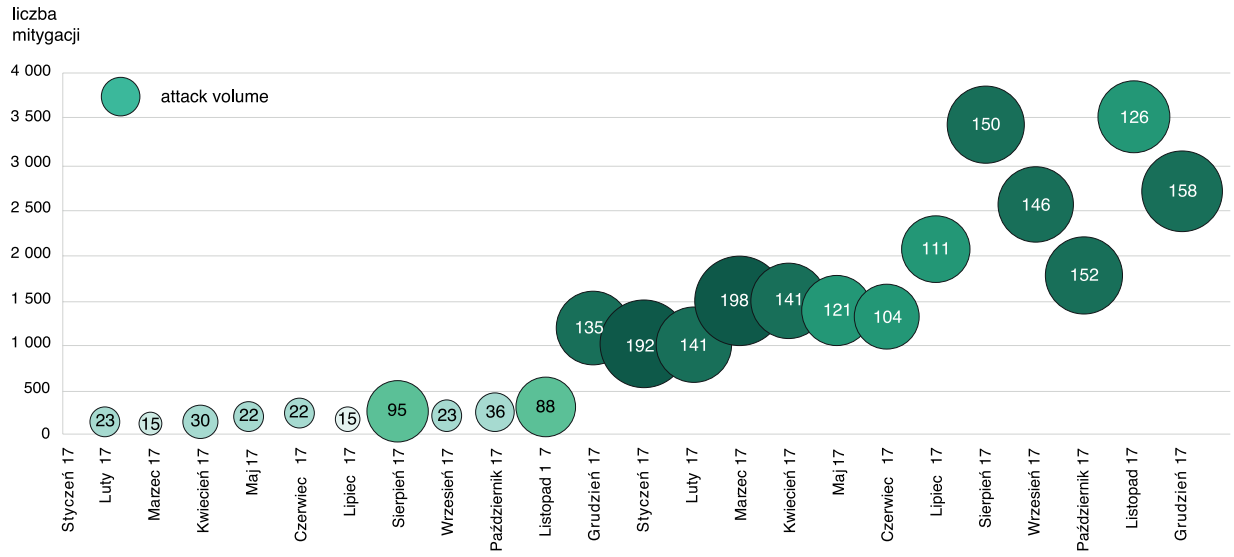
Ich głównym celem jest utrudnienie bądź uniemożliwienie korzystania z oferowanych przez zaatakowany system usług sieciowych, co w efekcie paraliżuje infrastrukturę ofiary poprzez masowe wysyłanie zapytań do zaatakowanej usługi.

Zgodnie z przewidywaniami, częstość występowania ataków DDoS nie maleje. W roku 2018 zarejestrowano ich znacznie więcej w porównaniu do roku 2017, choć na przestrzeni ostatnich lat częstość ich występowania utrzymuje się na zbliżonym poziomie. Podobnie jeśli chodzi o siłę ataków, która nieustanie rośnie. Średnia wielkość szczytowego natężenia ataku DDoS zaobserwowana w sieci Orange Polska sięgnęła poziomu 2,1 Gbps, znacznie wyższego niż w 2017 roku (ponad 1,2 Gbps). Z kolei największa odnotowana wartość natężenia ruchu w szczycie ataku to ok. 198 Gbps (przy 82 Gbps w 2017 r.).

Na wzrost siły ataków wpływ mają nie tylko szybsze łącza internetowe, ale też przystępna cena ataków DDoS na czarnym rynku oraz w dużym stopniu wykorzystywanie technik wzmocnionego odbicia oraz botnetów bazujących na urządzeniach internetu rzeczy.

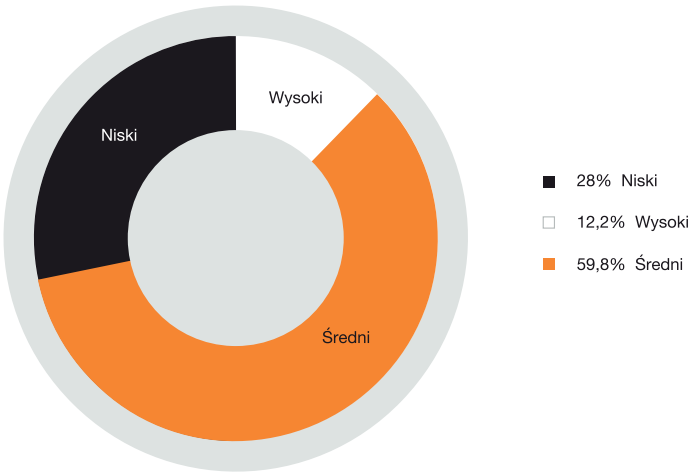
Ponad 97 procent wszystkich wykrytych w 2018 roku zdarzeń na urządzenia mobilne dotknęło systemu Android. Jego większa otwartość pozwalała twórcom złośliwego oprogramowania przygotować, przetestować i wprowadzić w obieg swój produkt o wiele łatwiej niż w przypadku systemu spod znaku jabłka.

Ataki odmowy dostępu do usługi (Distributed Denial of Service – DDoS) to jedne z najprostszych i najbardziej popularnych ataków na sieć lub system komputerowy, a zarazem jedne z bardziej niebezpiecznych i groźnych w skutkach.



Rysunek 3. *Liczba mitygacji (unieszkodliwiania) ataków DDoS.*

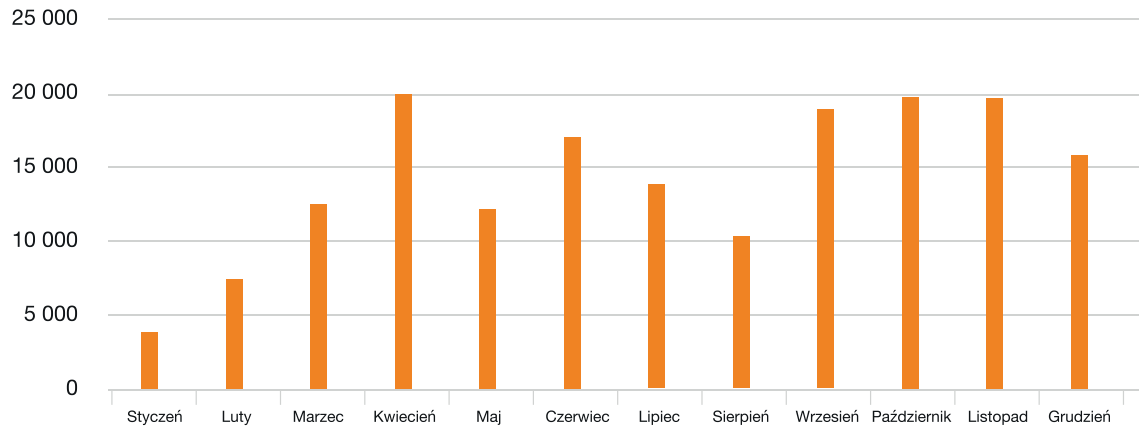
Warto również zwrócić uwagę na utrzymujący się od wielu lat trend, wskazujący na coraz krótszy czas trwania ataków. **Średni czas trwania wszystkich zarejestrowanych alertów w roku 2018 wyniósł ok.11 minut (15 minut w 2017 r.). Większość zarejestrowanych alertów, podobnie jak w 2017 roku, trwała poniżej 10 minut (blisko 88 proc. w roku 2018, nieco ponad 72 proc. w 2017 r.) – wzrost o 15 proc. w roku 2018.** Zjawisko to może być ściśle powiązane z licznymi atakami na użytkowników indywidualnych w związku z ich dużą aktywnością w sieci typu np. gry online (ataki skierowane przeciwko graczom online – wylogowanie gracza) oraz łatwiejszą dostępnością na czarnym rynku usług DDoS – im krótszy atak, tym bardziej dostępny (mniejszy koszt usługi).



Rysunek 4. *Diagram poziomu krytyczności alertów DDoS w rozkładzie procentowym.*

Już co czwarte szkodliwe zdarzenie w sieci (28%) to atak na urządzenia mobilne. Aż 97% z nich jest kierowane na system Android. Najczęściej atak przybiera formę złośliwej reklamy, tzw. malvertisement (43 proc.) i SMS-ów lub e-maili z linkami próbującymi wyłudzić pieniądze lub hasła do kont. Jak podkreślają eksperci CERT Orange Polska, wiele do życzenia pozostawiają również zabezpieczenia urządzeń internetu rzeczy, wykorzystywanych np. w inteligentnych domach, a także świadomość ich użytkowników.

W całym 2018 roku zespół CERT Orange Polska zrealizował łącznie 89 kampanii związanych z ochroną przed malware, którymi objętych zostało ponad 56 000 użytkowników CyberTarczy.



Rysunek 5. *Liczba zablokowanych e-maili ze szkodliwą zawartością w poszczególnych miesiącach 2018 r.*

Przeprowadziliśmy także 4 kampanie informacyjne poświęcone wyciekom haseł użytkowników Orange Polska. Kampaniami tymi objęliśmy ponad 13 000 klientów. Drugim wyraźnym trendem, obserwowanym w 2018 roku w sieci Orange Polska, jest aktywność oprogramowania typu Adware.

Jak chronić firmę małą i dużą przed zagrożeniami w sieci? Jak zabezpieczyć instytucję publiczną, a jak finansową? – wybrane usługi bezpieczeństwa Orange Polska.

Ochrona przed atakami DDoS

Ruch sieciowy jest monitorowany w trybie 24/7/365 pod kątem wykrywania anomalii. W przypadku faktycznego ataku filtrujemy podejrzane pakiety, a do klienta trafia jedynie prawidłowy ruch sieciowy. Wykorzystywane mechanizmy FlowSpec w sieci Orange pozwalają na przyjęcie i mitygację ataków wolumetrycznych o bardzo dużej wielkości.

Jak działa:

To połączenie trzech elementów: zespołów SOC i CERT Orange Polska, platformy Arbor Networks oraz wykorzystania mechanizmów operatorskich w ruchu krajowym i międzynarodowym (blackholing, zarządzanie konfiguracją routerów).

Korzyści:

- Zapewnienie dostępności usług w internecie
- Stały monitoring ruchu i identyfikacja wystąpienia potencjalnych zagrożeń
- Kompetencje specjalistów z Security Operations Center dostępne w trybie 24/7/365
- Natychmiastowe odparcie ataku od infrastruktury klienta
- Brak konieczności inwestowania w odpowiednią infrastrukturę i elastyczny model rozliczania

SOC as a Service

Gotowy proces monitorowania incydentów bezpieczeństwa przy wykorzystaniu kompetencji i zespołu Security Operations Center (SOC) Orange Polska – operatorów, analityków i ekspertów – monitorującego systemy i dane klienta np. poprzez SIEM.

Jak działa:

- Proces polegający na integracji danych z systemów klienta z zespołem szybkiego reagowania na zidentyfikowane incydenty
- Dostarczenie kompletnego rozwiązania, w celu monitorowania w trybie 24/7/365, integracja źródeł logów, opracowanie i wdrożenie scenariuszy bezpieczeństwa

Korzyści:

- Dostępne procedury obsługi incydentów
- Doświadczony zespół specjalistów
- Brak konieczności budowania od podstaw zespołu specjalistów i kompetencji po stronie klienta
- Natychmiastowe informowanie osób odpowiedzialnych za infrastrukturę i dane chronione o incydentach
- Stałe monitorowanie i identyfikacja incydentów bezpieczeństwa
- Gotowe zestawy scenariuszy bezpieczeństwa dla systemów klienta
- Centralna baza wiedzy o monitorowanych systemach
- Elastyczny model szyty na miarę, tzn. możliwość uruchomienia u klienta lub w modelu chmurowym

email Protection

Ochrona poczty klienta przed infekcjami, phishingiem, spamem i wyciekiem danych.

Jak działa: Polega na wykorzystaniu gotowej platformy w sieci Orange Polska.

Korzyści:

- Ochrona informacji przekazywanych drogą elektroniczną
- Rozwiązanie nie wymaga inwestycji w infrastrukturę po stronie klienta
- Brak inwestycji w infrastrukturę po stronie klienta
- Scentralizowana polityka bezpieczeństwa dla wszystkich chronionych lokalizacji

MDM

Monitorowanie i zarządzanie urządzeniami mobilnymi klienta, np. smartfony, tablety.

Jak działa:

- Zarządzanie flotą mobilną poprzez konsolę
- Centralne zarządzanie:
  - urządzeniami mobilnymi - lokalizacja, konfiguracja, backup, zdalne blokowanie, czyszczenie danych
  - aplikacjami – centralne repozytorium aplikacji, zdalna dystrybucja i instalacja aplikacji dla grup użytkowników
  - tworzeniem kopii zapasowych najważniejszych danych dostępnych na urządzeniu mobilnym
  - polityką bezpieczeństwa
  - zdalnym wsparciem technicznym

Korzyści:

- Centralne zarządzanie urządzeniami mobilnymi w firmie
- Standaryzacja

CyberTarcza as a Service

Ochrona urządzeń mobilnych klienta działających w sieci Orange Polska przed złośliwym oprogramowaniem oraz kampaniami phishingowymi.

Jak działa: Działa w oparciu o analizę ruchu sieciowego operatora, bez względu na system.

Funkcjonalności:

- Antymalware, antyphishing
- Możliwość zdefiniowania blokad w różnych godzinach dla pracowników i rodziny

CyberTarcza zawiera dodatkowe źródła danych o zagrożeniach, opracowane pod kątem klienta, oraz umożliwia użytkownikowi zarządzanie filtrami, ponad 30 kategorii.

Korzyści:

- Możliwość filtrowania
- Ochrona przed cyberzagrożeniami typu APT i zero-day
- Brak konieczności inwestowania w urządzenia zabezpieczające usługi
- Ochrona przed niefrasobliwością pracowników klienta

Cały Raport CERT Orange Polska do pobrania

https://www.cert.orange.pl/aktualnosci/raport-cert-orange-polska-za-2018-rok