Bezpieczny biznes
z Orange Network Security

#cyfroweewolucje

orange™

Cyfrowe ewolucje firm

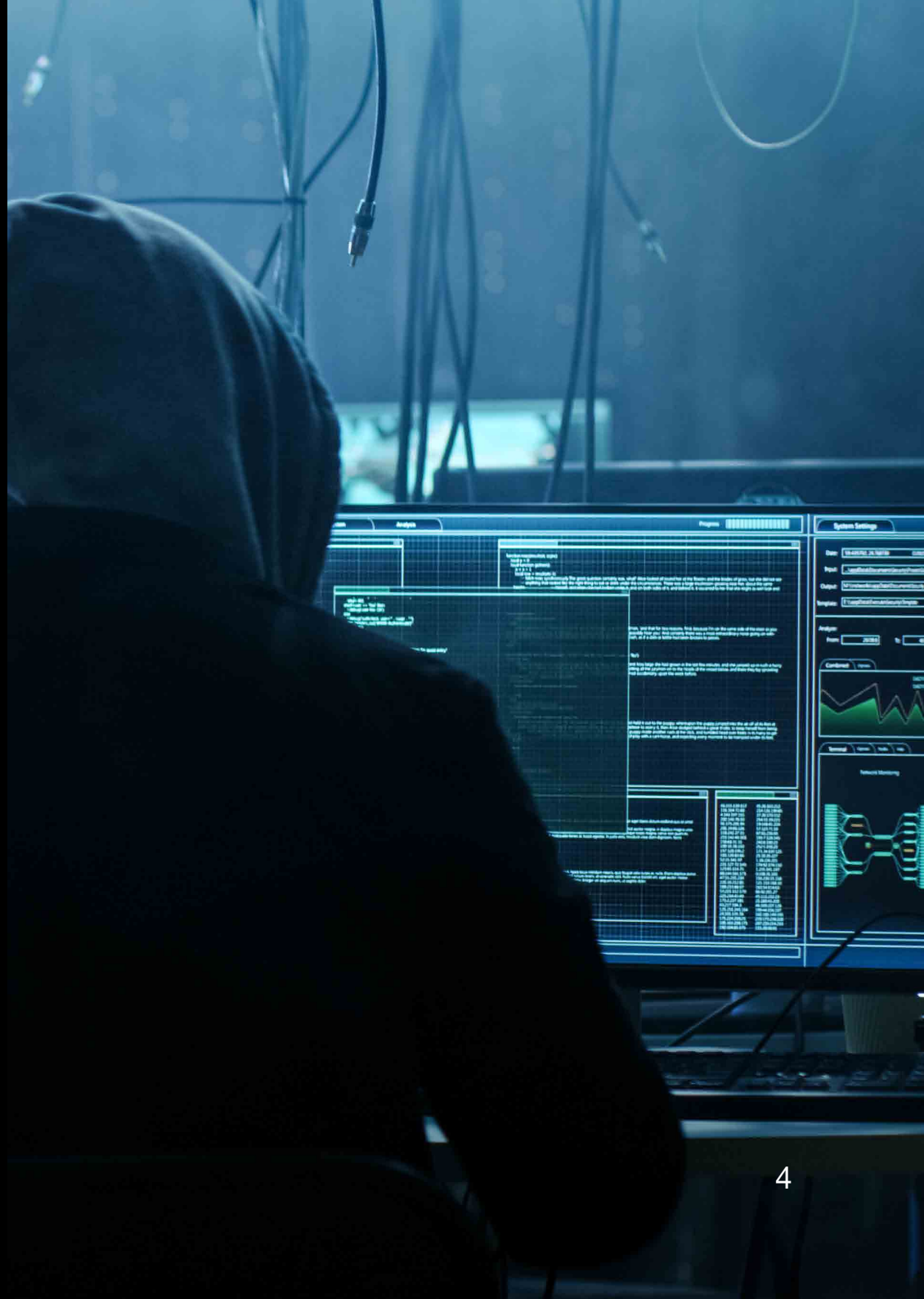
Rewolucja cyfrowa dzieje się na naszych oczach. Obejmuje kolejne sektory gospodarki, ale wkracza również w życie publiczne i prywatne. Staje się przedmiotem dyskusji i analizy ekspertów. Jest niepodważalna, tak samo jak fakt, że z jednej strony niektóre branże lub firmy straciły rację bytu, z drugiej powstały nowe, będące odpowiedzią na współczesne potrzeby konsumentów.

W biznesie jednak nikt nie lubi rewolucyjnych zmian. Bo mogą one przynieść zyski, ale mogą także przynieść katastrofalne koszty. W biznesie ważniejszy jest rozwój w oparciu o solidną strategię. Dotyczy to zarówno wielkiej korporacji, jak i lokalnej pizzerii.

Jak zwiększyć bezpieczeństwo korzystania z internetu, chronić infrastrukturę i zapewnić ciągłość działania firmy bez kosztownych inwestycji, opierając się na rozwiązaniach, wiedzy i doświadczeniu operatora telekomunikacyjnego?

Cyberbezpieczeństwo staje się biznesowym priorytetem

Dostęp do internetu to dzisiaj fundament działania praktycznie każdej firmy. Połączenie z siecią oznacza jednak otwarcie się na potencjalne zagrożenia związane z cyberatakami. Trzeba chronić się przed włamaniami, złośliwym oprogramowaniem, phishingiem, kontrolować działania pracowników i dysponować narzędziami wczesnego ostrzegania i reagowania - koszty błędów czy niedopatrzeń bywają ogromne.

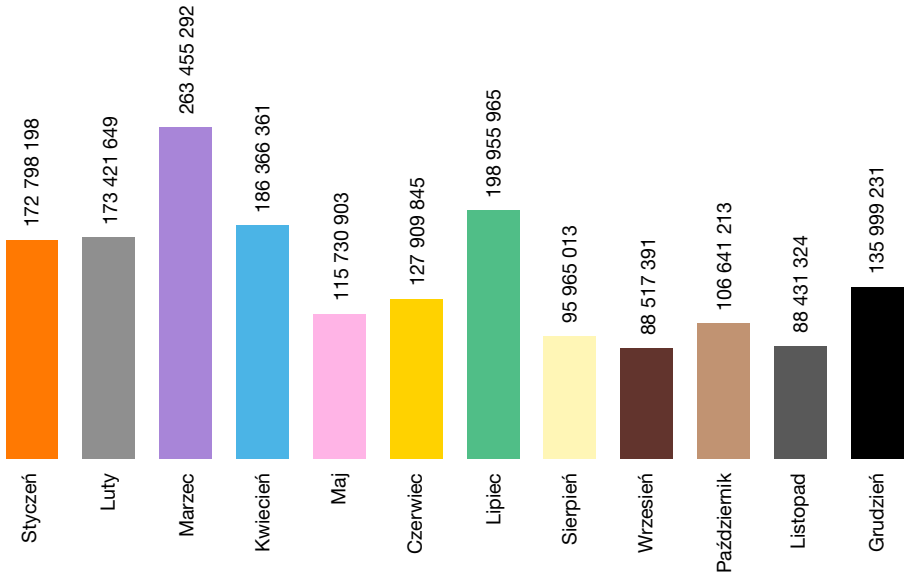


Praktycznie co tydzień można przeczytać o nowych spektakularnych cyberatakach na globalne i lokalne organizacje, instytucje finansowe, w tym giełdy, a także administrację publiczną. Ataki ransomware mogą skutecznie zablokować funkcjonowanie nawet największych firm, a czasem kończą się dopiero z chwilą zapłacenia liczonego w milionach dolarów okupu. Niestety, nawet jeśli zapłacimy okup, nie mamy gwarancji, że przestępcy zwrócą nasze dane. Koszty popularnych ataków DDoS (Distributed Denial of Service) dla przestępców to zaledwie od kilkunastu do kilkuset dolarów za kampanię, natomiast dla przedsiębiorstw oznaczają czasem ogromne straty – nie tylko finansowe, liczone w tysiącach czy nawet milionach dolarów, ale również wizerunkowe.

Polska nie jest zieloną cyberwyspą

Polska nie stanowi pod tym względem wyjątku na mapie świata. Raport CERT Orange Polska za rok 2019 wskazuje kilka spektakularnych przykładów ataków na polskie organizacje. W lutym ubiegłego roku ofiarą phishingu padł potentat z branży zbrojeniowej. Koszt? 4 mln zł. Efektem wycieku danych z jednego z popularnych sklepów internetowych była nałożona we wrześniu kara w wysokości 3 mln zł. Po ataku ransomware na jeden z urzędów gminy systemy i usługi do pełnej operacyjności zostały przywrócone po kilku tygodniach. Nikt nie może spać spokojnie - przestępcy atakują nawet organizacje charytatywne, które pomagają chorym dzieciom.

Phishing. Liczba interwencji CyberTarczy w rozkładzie miesięcznym:



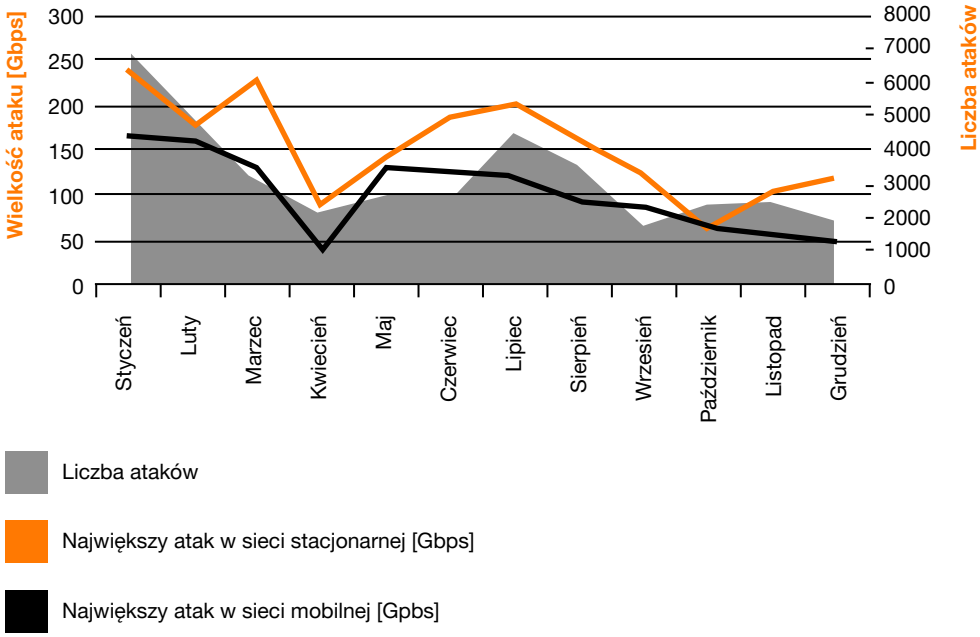
Średnio

4 806 007 zdarzeń dziennie

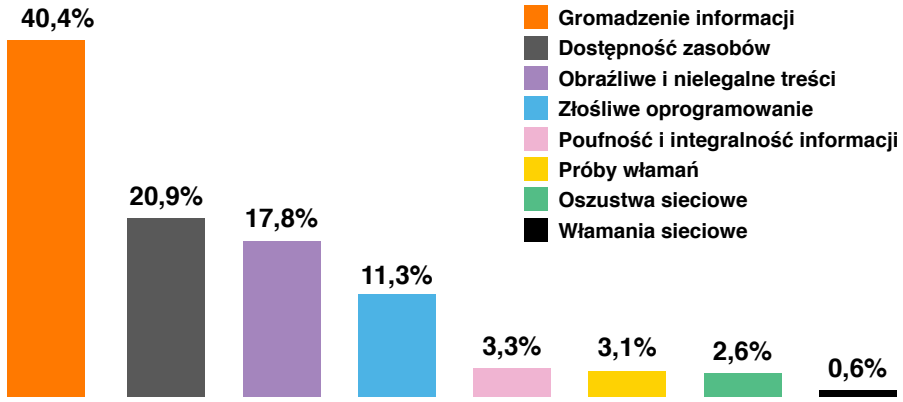
Phishing, czyli próby wyłudzania wrażliwych danych, w sieci Orange Polska stanowiły w ubiegłym roku już ponad 40% wszystkich zagrożeń, podczas gdy rok wcześniej ich udział wynosił zaledwie 21%. Udaje się je wykrywać i zapobiegać im dzięki usługom takim jak Orange Network Security, ale skala zjawiska jest niepokojąca. Rośnie popularność smishingu, czyli ataków phishingowych za pomocą SMS-ów. Tylko w pierwszym kwartale tego roku CERT Orange Polska obsłużył o około jedną czwartą więcej incydentów niż w tym samym czasie rok wcześniej. Przypadków dotyczących phishingu i scamu było aż o 44% więcej niż w tym samym okresie roku ubiegłego.

Wciąż powszechne są ataki DDoS - stanowiły w zeszłym roku 21% wszystkich zagrożeń - których celem jest m.in. zablokowanie serwisu internetowego czy zdalnego dostępu do sieci (w tym możliwości pracy zdalnej) poprzez zalanie go olbrzymim ruchem. Największy - stwierdzony 12 czerwca 2020 roku w sieci Orange i oczywiście skutecznie odparty - atak DDoS w historii polskiego internetu miał 303 gigabity na sekundę i 88 milionów pakietów na sekundę.

Liczba oraz wolumen ataków DDoS w 2019 roku:



Rozkład procentowy kategorii incydentów obsłużonych przez CERT Orange Polska w 2019 roku:

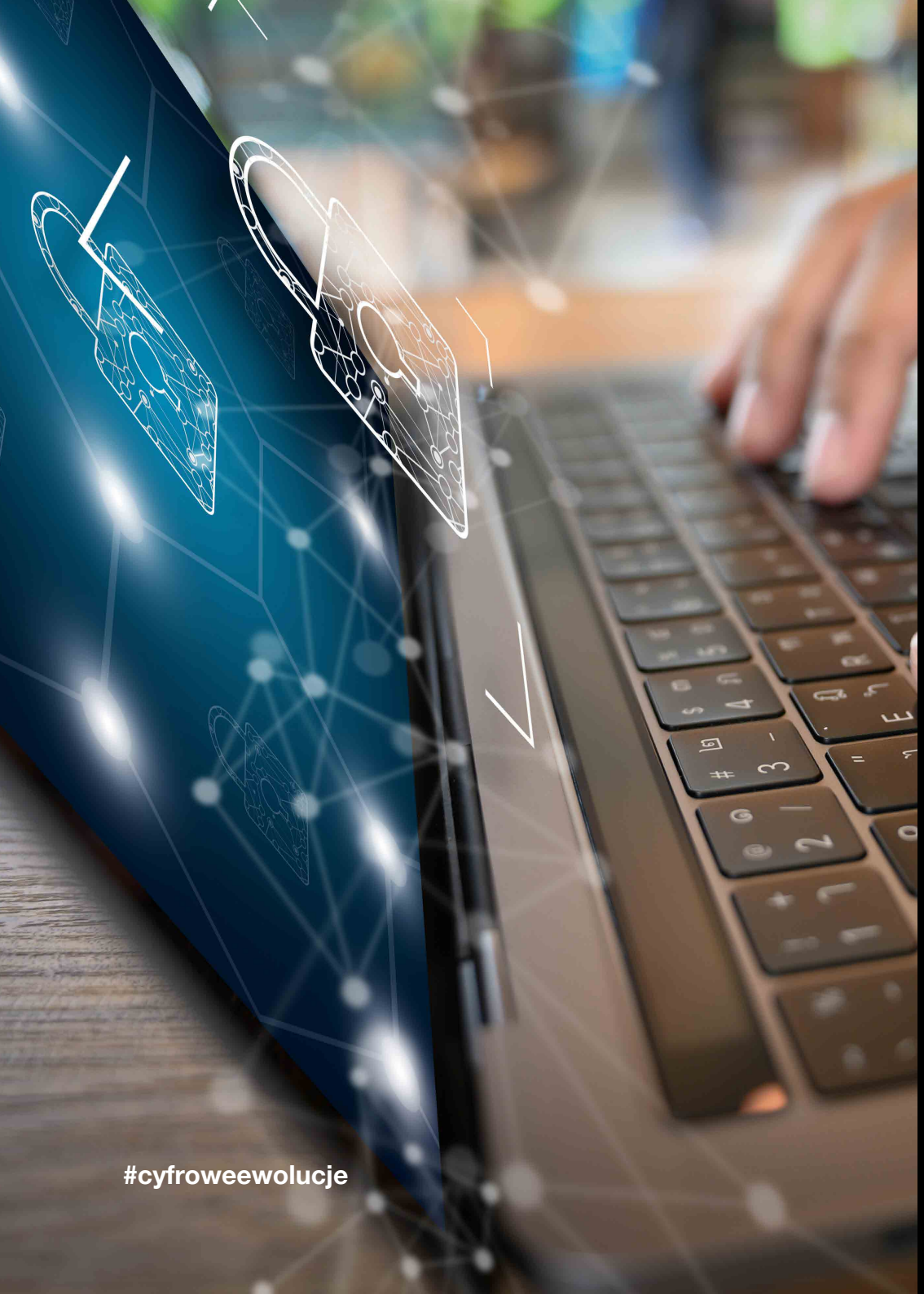


Poziom cyberzagrożenia dla firm systematycznie rośnie i nic nie wskazuje, że miałoby się to zmienić na lepsze. Zespół CERT Orange Polska przewiduje, iż zagraniczne sukcesy sprawią, że wkrótce przestępcy będą masowo atakować firmy za pomocą ransomware również w Polsce. Celem cyberataków staną się nowe usługi i rozwiązania bazujące na otwartej bankowości. Coraz częściej wykorzystywane jako wektor ataków phishingowych i dystrybucji złośliwego oprogramowania będą także aplikacje webowe w chmurze.

Bądź gotowy na wszystko! Ale jak to zrobić?

Ochrona przed zagrożeniami jest tym trudniejsza, że krajobraz cyberbezpieczeństwa nieustannie się zmienia. Przygotowanie się na potencjalne zagrożenia wymaga znacznych inwestycji w technologię i ludzi. Dostęp pracowników do firmowej infrastruktury trzeba zabezpieczyć przy pomocy sieci VPN, prywatnych APN i nowoczesnych zapór ogniowych. Należy nieustannie edukować pracowników, a przy tym mieć doświadczony zespół wysoko wykwalifikowanych specjalistów, który będzie w stanie nadzorować zabezpieczenia techniczne i obsłużyć incydenty. Jest to coraz trudniejsze w dobie globalnych kryzysów, w obliczu wzrostu ilości i jakości zagrożeń oraz ograniczonych budżetów. Do cyberbezpieczeństwa można podejść jednak inaczej, nowocześniej, bardziej ekonomicznie, usługowo. Orange oferuje kompleksową, integrującą sieci mobilne i stacjonarne, ochronę wbudowaną w usługi dostępu do internetu oraz transmisji danych.

#cyfroweewolucje



Usługa Orange Network Security zapewnia wszechstronną ochronę

Orange Network Security (ONS) to elastyczna platforma bezpieczeństwa w chmurze, która umożliwia szczegółową kontrolę wykorzystania internetu. Klient otrzymuje rozwiązanie podnoszące poziom bezpieczeństwa bez konieczności instalowania jakiegokolwiek urządzenia w swoich lokalizacjach.

Usługa Orange Network Security składa się z dwóch głównych komponentów:

- **systemu Next Generation Firewall** służącego do ochrony ruchu przychodzącego i wychodzącego umieszczonego w infrastrukturze Orange Polska,

- **portalu** wykorzystywanego do zarządzania usługą przez klienta.

Cała komunikacja w internecie przechodzi przez ONS i jest kontrolowana zgodnie z zakresem funkcjonalnym wykupionego pakietu:

- **Zapora ogniowa (firewall)** – ochrona całego ruchu przychodzącego i wychodzącego,
- **Kontrola aplikacji oraz Web Filtering** – kontrola wykorzystania internetu oraz korzystania z aplikacji, zezwalanie lub blokada dostępu do stron WWW oraz aplikacji,
- **Antywirus (antymalware)** – ochrona przed znanymi zagrożeniami: wirusami, trojanami, robakami internetowymi,
- **Antybotnet** – wykrywanie zainfekowanych komputerów, nad którymi kontrola może zostać przejęta przez cyberprzestępców, komputery mogą stać się źródłem ataku DDoS lub innego,
- **Intrusion Prevention System (IPS)** – ochrona przed włamaniami do sieci i serwerów,
- **Sandbox** – ochrona przed nieznanymi zagrożeniami.

Usługa oferowana jest w postaci pakietów bezpieczeństwa:

- **Basic** – Firewall, Web Filtering, kontrola aplikacji, raportowanie,
- **Standard** – zakres pakietu Basic plus Antywirus, IPS,
- **Premium** – zakres pakietu Standard plus Sandbox.

Jakie korzyści zapewnia ONS?

Optymalne rozwiązanie bezpieczeństwa IT – bezpieczny dostęp do internetu i kontrola jego wykorzystania, wysoka skuteczność i dostępność, w postaci ekonomicznej usługi, bez konieczności inwestowania w sprzęt oraz konieczności jego utrzymania.

Szeroki zakres funkcjonalności: od zapory ogniowej przez kontrolę aplikacji po ochronę przed złośliwym oprogramowaniem – różne rodzaje ataków cyberprzestępców są odpierane, zanim dotrą do firmowych systemów. Kombinacja funkcji Antybot, IPS, Antywirus, Sandbox pozwala na wzmocnienie ochrony przed podejrzaną działalnością, wykrywając komputery, które mogą być źródłem ataku, np. DDoS.

Wdrażając elastyczną usługę ONS, można zapewnić **odpowiednią wydajność**, przy posiadaniu **jednolitej polityki bezpieczeństwa** dla ochrony wszystkich danych i sieci.

#cyfroweewolucje

Prosty i przyjazny dla użytkownika portal umożliwia klientowi zarządzanie rozwiązaniem online. Zarządzanie usługą ONS odbywa się online w czasie rzeczywistym z wykorzystaniem Portalu ONS. Można także korzystać ze wsparcia Orange dla Firm, zlecając zmiany konfiguracji usługi wykwalifikowanym służbom OPL.

Narzędzia konfiguracyjne do kontroli aplikacji i filtrowania sieci WWW - umożliwiają wybór, jakiego rodzaju aplikacje lub strony internetowe są udostępnione użytkownikom, do których mają mieć dostęp i chronią przed podejrzanym działaniem.

ONS dostarcza informacji o działaniu usługi w postaci **raportów pozwalających na wizualizację TOP witryn i aplikacji** odwiedzanych przez użytkowników. W tym samym raporcie prezentowane są informacje o **wykrytych zagrożeniach** typu botnet, malware i innych.

Niezawodność ciągłego działania jest wsparta gwarantowaną dostępnością na poziomie 99,99%, co oznacza maksymalnie 4 minuty niedostępności w skali miesiąca. Za poprawność działania usługi i aktualizacje odpowiada w całości **Orange Polska**. Bezpośrednią kontrolę nad ONS sprawuje doświadczony zespół CERT Orange Polska.

Kto powinien zainteresować się ONS?

Cyberbezpieczeństwo jest dzisiaj priorytetem dla wszystkich organizacji, ale szczególnego znaczenia nabiera dla dużych przedsiębiorstw, instytucji oraz międzynarodowych korporacji – to właśnie one bardzo często stanowią cel ataków zarówno tych mniej, jak i bardziej doświadczonych przestępców.

ONS to propozycja skierowana do organizacji zainteresowanych przede wszystkim ekonomicznym, a zarazem elastycznym, umiejscowionym w chmurze Orange rozwiązaniem cyberbezpieczeństwa, które pozwoli zaspokoić potrzeby w zakresie:

Ochrony infrastruktury
Wykrywanie złośliwych zachowań. Jednolita polityka bezpieczeństwa dla całej firmy (fix & mobile).

Bezpiecznego korzystania z internetu
Ochrona wykorzystania internetu. Ochrona przed włamaniami, wirusami i wszelkiego rodzaju innymi cyberzagrożeniami.

Kontroli wykorzystania internetu
Kontrola właściwego wykorzystania internetu przez pracowników. Filtrowanie dostępu do zabronionych aplikacji oraz stron.

Zapewnienia ciągłości biznesowej
Ochrona aplikacji. Wysoka dostępność usługi - 99,99%.

Dlaczego Orange?

Jedna oferta, jeden dostawca usług Internet & Data & Security, jedna odpowiedzialność

Operatorzy telekomunikacyjni są na pierwszej linii walki z cyberzagrożeniami. Orange Polska ma w zakresie ochrony ponad 20-letnie doświadczenie Działający w jego strukturach zespół Computer Emergency Response Team (CERT) to specjalistyczna jednostka, która jest odpowiedzialna za bezpieczeństwo użytkowników internetu, korzystających z sieci operatora. Blisko 80 ekspertów monitoruje w trybie ciągłym 24/7 zagrożenia dla bezpieczeństwa systemów podłączonych do sieci Orange Polska i reaguje na wykryte zagrożenia, w tym na incydenty zgłaszane przez użytkowników sieci. Dwie dekady doświadczeń oraz zasięg monitoringu – niemal 40% całego polskiego internetu - sprawiają, że zespół CERT Orange Polska wie i widzi znacznie więcej.

Prawie

11,5 mln

zablokowanych prób wejścia na strony phishingowe

Przeszło

2,5 mln

klientów ochronionych przed działaniem złośliwego oprogramowania

Te liczby ilustrują mozolną pracę zespołu CERT Orange Polska. Na co dzień niewidoczną, jednak bezpośrednio przekładającą się na poczucie bezpieczeństwa naszych klientów. *

* Dane z 2019 roku

W ciągu każdej godziny na statystycznego użytkownika internetu w sieci Orange nakierowanych jest kilkanaście prób ataków z całego świata. Łącznie oznacza to kilka milionów ataków na dobę. W czasie rzeczywistym ekspertów w akcji, działanie technologii zainstalowanych w Orange oraz informacje o najczęstszych atakach można obserwować na Mapie Zagrożeń dostępnej na stronie https://www.cert.orange.pl/mapa

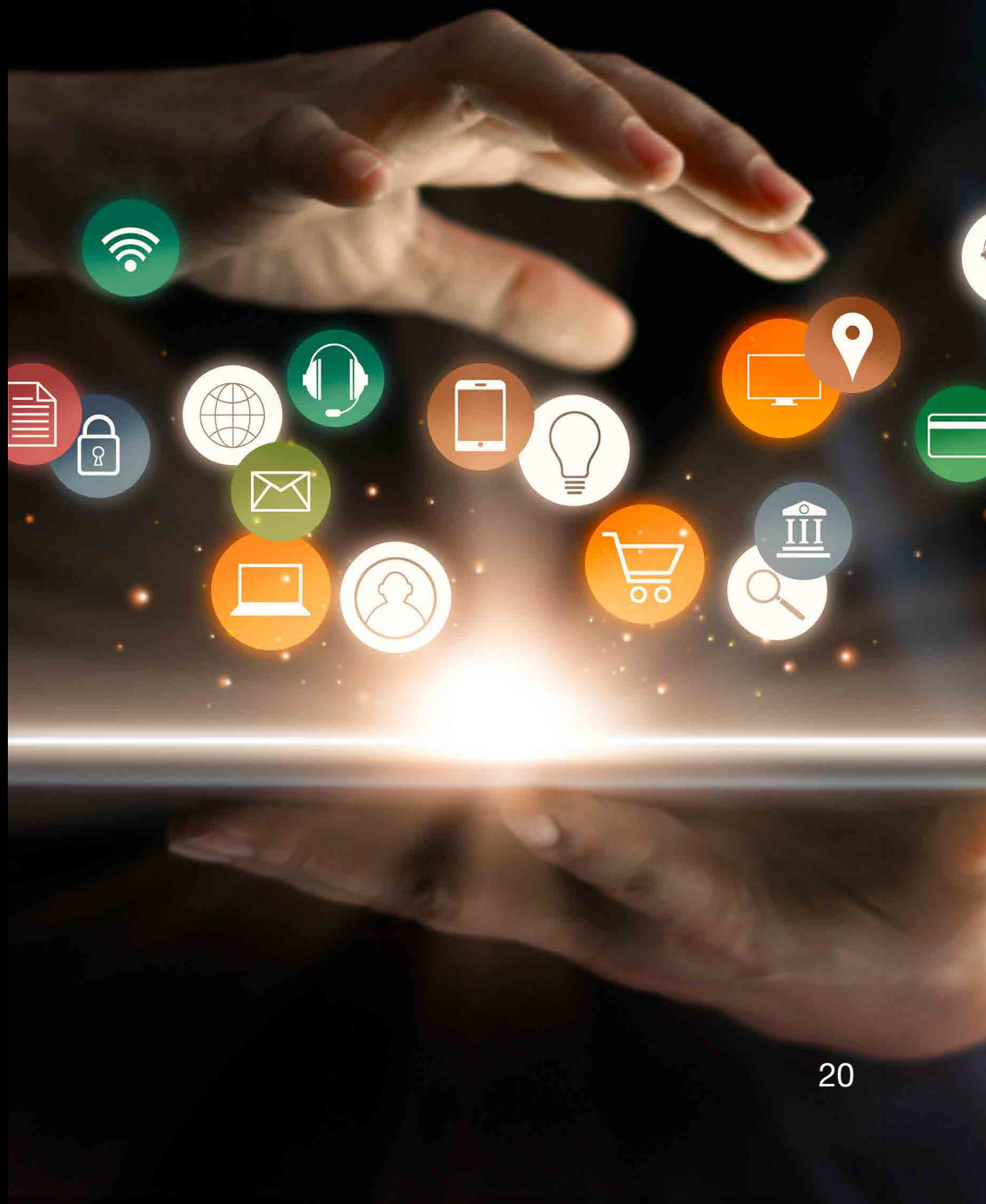
Orange ma kompleksową ofertę dla dużych organizacji, na którą składają się nie tylko usługi telekomunikacyjne, ale także rozwiązania takie jak Biznesowy VPN (umożliwia połączenie oddziałów firmy klienta w bezpieczną sieć transmisji danych), Miejski Ethernet (ultraszybki dostęp do internetu oraz wysokie parametry transmisji danych) czy Prywatny APN w Orange (umożliwia szybką i bezpieczną komunikację różnych urządzeń mobilnych, korzystających z sieci komórkowej ze środowiskiem danych i aplikacji firmowych) – a wszystko to wzbogacone jest o zaawansowane usługi cyberbezpieczeństwa, takie jak ONS.

ONS w praktyce: prosta, błyskawiczna, elastyczna

Usługa jest bardzo prosta w instalacji i konfiguracji. W związku z tym, że działa w oparciu o infrastrukturę Orange i nie wymaga zakupu dodatkowego sprzętu, można ją uruchomić błyskawicznie. Wystarczy kilka godzin, żeby objąć ochroną własną infrastrukturę, użytkowników i cały swój biznes.

Usługa jest w pełni skalowalna. Oznacza to, że klient nie musi poświęcać czasu na wymiarowanie infrastruktury bezpieczeństwa. Dokonując upgrade'u, nie trzeba kupować kolejnych urządzeń – wszystko co potrzebne zainstalowane zostało w chmurze Orange.

Nie trzeba się przy tym martwić o funkcjonowanie usługi. Orange dla Firm gwarantuje wysoką dostępność na poziomie czterech dziewiątek (99,99%).



ONS dostępna jest przede wszystkim w postaci trzech pakietów (Basic, Standard i Premium), ale możliwe jest równocześnie bardziej precyzyjne dopasowanie usługi, a nawet wzbogacenie jej o dodatkowe elementy na żądanie klienta. W ten sposób oferowane są rozwiązania „szyte na miarę", negocjowane i wyceniane indywidualnie, dostępne w postaci dedykowanego projektu technicznego dla użytkowników ONS. Dotyczy to elementów funkcjonalnych, takich jak np.:

DMZ – czyli strefa zdemilitaryzowana, w której znajdują się udostępniane zasoby, to dodatkowa warstwa bezpieczeństwa dla lokalnej infrastruktury sieciowej, która jest chroniona przez zaporę ogniową.

IPsec VPN oraz SSL VPN – możliwość udostępniania urządzeń za pośrednictwem szyfrowanych wirtualnych sieci prywatnych.

Integracja z AD – integracja z usługami katalogowymi pozwala na tworzenie i stosowanie zróżnicowanej polityki bezpieczeństwa, dopasowanej do poszczególnych grup użytkowników, np. pracowników poszczególnych oddziałów czy ze względu na specyfikę wykonywanych obowiązków.

Tak jak rozwija się obszar cyberbezpieczeństwa, pojawiają się nowe rodzaje ataków oraz nowe technologie pozwalające im zapobiegać, tak vusługa ONS jest konsekwentnie rozwijana o nowe funkcjonalności.
W planach Orange znajduje się m.in.:

- uruchomienie usługi dla pasm powyżej 300 Mb/s

- dedykowany wirtualny system Next Generation Firewall

- inspekcja SSL z wykorzystaniem rozszyfrowywania SSL

#cyfroweewolucje

Case study

Wyzwanie: kilkadziesiąt biur i placówek w całej Polsce – duża firma z sektora handlu detalicznego poszukiwała skutecznego, a zarazem ekonomicznego sposobu podniesienia poziomu bezpieczeństwa swojej sieci i ochrony wykorzystania internetu przez pracowników.

Rozwiązanie: organizacja wybrała usługę Orange Network Security w wersji Premium – kompleksowe rozwiązanie umiejscowione poza infrastrukturą klienta, w chmurze Orange, pozwoliło na zwiększenie bezpieczeństwa wykorzystania internetu i zachowanie pełnej kontroli nad własną polityką bezpieczeństwa. Elastyczna platforma bezpieczeństwa do ochrony przeglądania internetu w całej firmie została zintegrowana z polityką bezpieczeństwa ustaloną dla poszczególnych lokalizacji wspólnie - przez Orange i klienta.

Korzyści:

Kontrola - realizacja kontroli praw dostępu oraz wykorzystania internetu przez pracowników bez konieczności instalacji sprzętu we własnej infrastrukturze,

Efektywność ekonomiczna - elastyczny model finansowania zapewnia pełną kontrolę nad kosztami i gwarantuje, że opłaty ponoszone są wyłącznie za to, co jest potrzebne i faktycznie wykorzystywane,

Elastyczna ochrona - narzędzia do kontroli aplikacji i filtracja WWW pozwala na decydowanie, jakie rodzaje aplikacji lub jakie kategorie stron są dostępne dla użytkowników lub grup użytkowników,

Ochrona infrastruktury - Antybot, IPS oraz Antywirus pozwalają na wzmocnienie ochrony przed podejrzaną działalnością, zapewnienie ciągłości biznesowej – ochrona aplikacji i gwarancja wysokiej dostępności ONS.

Więcej informacji o Orange Network Security
www.orange.pl/duze-firmy/orange-network-security