

Orange Network Security czyli bezpieczeństwo Twojej firmy

Usługa Orange Network Security umożliwia filtrowanie stron WWW oraz kontrolę nad wszelkimi wysyłanymi i odbieranymi danymi w każdym oddziale firmy. Orange Network Security to jednocześnie firewall, możliwość bardzo szybkiego przesyłania informacji między lokalizacjami oraz bezpieczeństwo w postaci zapasowego łącza.

Porównanie kosztów cyberataków do kosztu tarczy antykryzysowej w związku z COVID we Francji:

530 mld euro – straty wygenerowane w 2019 r. przez globalne cyberataki

300 mld euro – koszt tarczy antykryzysowej po pandemii koronawirusa we Francji

Statystyki dotyczące cyberataków:

44% polskich firm poniosło straty finansowe na skutek cyberataków

70% firm miało przynajmniej jedno naruszenie danych z powodu źle chronionych urządzeń

Najczęstsze konsekwencje ataków:



Wyciek danych chronionych

Możliwe konsekwencje prawne i kary wynikające z RODO oraz straty wizerunkowe.



Przestoje i zakłócenia w funkcjonowaniu firmy

Przerwy w pracy i koszty z nich wynikające.



Zaszyfrowanie i kradzież danych (ransomware)

Koszty prawne dochodzenia i poradzenia sobie z szantażystami oraz konieczność wdrożenia środków zapobiegawczych.

Z czego wynika niedostateczne zabezpieczenie firm?



Niedocenianie zagrożenia i nieuwzględnienie go w strukturze firmy

Tylko 20% polskich przedsiębiorstw ma specjalistę ds. bezpieczeństwa w sieci.



Brak rozwiązań i procedur koniecznych do szybkiego reagowania w przypadku cyberataku

46% spółek nie ma operacyjnych procedur reakcji na incydenty.



Brak zrozumienia nowoczesnego środowiska wirtualnego i postrzeganie jako źródła ataków jedynie komputerów

54% przedsiębiorców główne źródło zagrożeń widzi w komputerach, a tylko 6% dostrzega je np. w urządzeniach wielofunkcyjnych.



Brak wiedzy o istniejących zintegrowanych rozwiązaniach dostarczanych przez certyfikowanych partnerów.

Firmy obawiają się, że koszty zabezpieczenia przed cyberprzestępczością mogą być wysokie i dlatego przeznaczają na nie średnio tylko 3% budżetu.

Tymczasem skutki ignorowania zagrożeń mogą być rujnujące.

3 głośne naruszenia cyberbezpieczeństwa z ostatnich miesięcy:

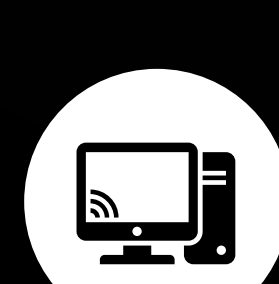


Troska o firmową sieć i dane Twoich klientów czy pracowników jest kluczowa.

Twoja firma potrzebuje czterech płaszczyzn ochrony:

Ochrona infrastruktury

- Wykrywanie złośliwych zachowań
- Zintegrowana polityka bezpieczeństwa całej firmy



Kontrola wykorzystania internetu

- Kontrola wykorzystania sieci przez pracowników
- Filtracja stron i aplikacji

Bezpieczne korzystanie z internetu

- Ochrona codziennej pracy w sieci
- Ochrona przed włamaniami i wirusami



Zapewnienie ciągłości biznesowej

- Ochrona kluczowych narzędzi i aplikacji
- Stała dostępność pomocy i usług



Wszystkie te potrzeby zapewnia Orange Network Security.

Źródła: Raport „Cyber-ruletka po polsku” PwC Polska • Niebezpiecznik.pl • Ministerstwo Cyfryzacji

Skorzystaj z wiedzy i doświadczenia Orange dla Firm

- partnera cyfrowej transformacji

www.orange.pl/view/network-security

