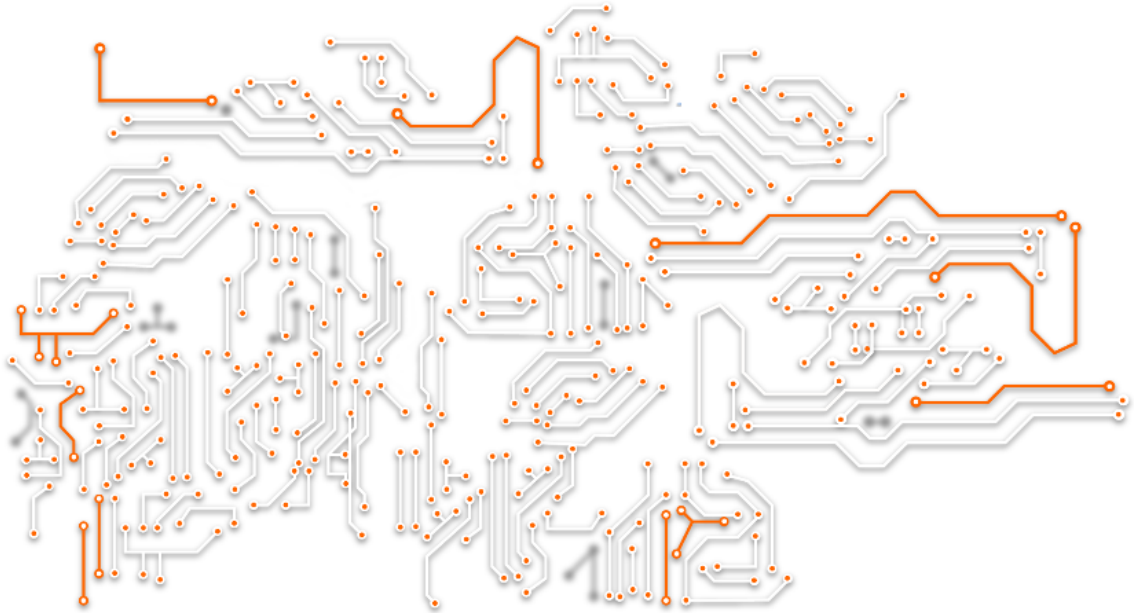

orange™

Raport
CERT Orange Polska



sieć Orange Polska 2014

- ponad 2 miliony klientów stacjonarnych usług szerokopasmowego dostępu do internetu
- ponad 1,5 miliona klientów usług szerokopasmowego mobilnego internetu
- efektywna identyfikacja zagrożeń
- skuteczna mitygacja ryzyk
- kompetentny zespół ekspertów bezpieczeństwa SOC/CERT
- stały monitoring poziomu bezpieczeństwa użytkowników sieci 24/7/365

SOC / CERT Orange Polska

- pierwszy polski telekom certyfikowany przez Computer Emergency Response Team (CERT®)
- Operacyjne Centrum Bezpieczeństwa (SOC)
- pierwsze komercyjne Security Operations Center w Polsce (2010)
- pierwsza komercyjna usługa DDoS Protection (2012)

bezpieczeństwo w liczbach

- 18 lat doświadczenia
- 70+ certyfikatów: (m.in. CISA, CISM, CISSP, SABSA, ITIL, ISO, Juniper, Sourcefire/Cisco, HP ArcSight, CheckPoint, Crossbeam/BlueCoat, McAfee/Intel, PaloAlto, F5)

incydenty obsługiwane przez SOC OPL*

* średnie miesięczne dane 2014

edukacja i podnoszenie świadomości

publikujemy alerty bezpieczeństwa oraz praktyczne informacje budujące świadomość bezpiecznych zachowań w sieci

- oferujemy dla najmłodszych "bezpieczny starter"

- udostępniamy poradnik dla rodziców

- alerty bezpieczeństwa dostępne on-line na stronie cert.orange.pl

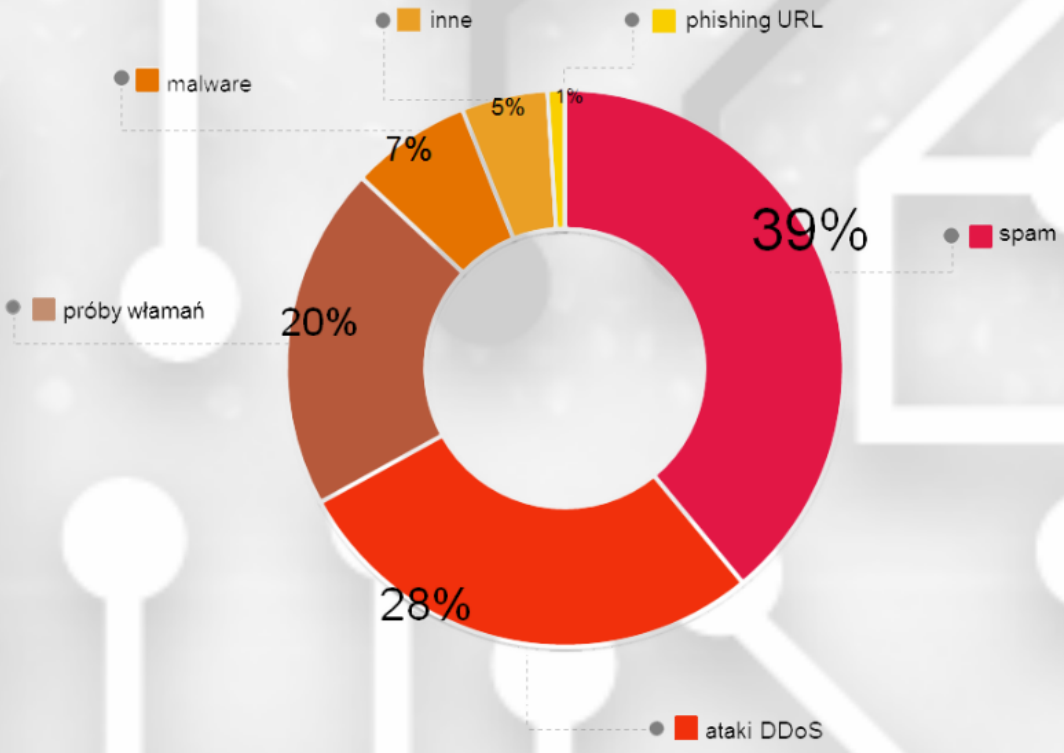
- jesteśmy aktywni w sieci "blog Orange Polska"

mamy wpływ na poziom bezpieczeństwa teleinformatycznego

- minimalizacja zagrożenia związanego z atakami na modemy DSL klientów (około 94 tys. podatnych modemów, około 44 tys. zaatakowanych urządzeń)
- analizy malware, blokowanie komunikacji zainfekowanych stacji użytkowników z serwerami C&C
- blokowanie dostępu do domen phishingowych oraz zawierających złośliwe oprogramowanie
- skuteczne mitygacje ataków DDoS
- podsumowanie ubiegłorocznych działań oraz najważniejsze wnioski w Raporcie CERT Orange Polska

CERT Orange Polska - rok 2014

- ok. 1 000 - miesięczna liczba obsłużonych incydentów bezpieczeństwa
- 100 tys. - liczba alertów dotyczących potencjalnych ataków DDoS
- ok. 40% - wzrost liczby alertów DDoS w porównaniu z 2013
- 93 Gbps (gigabitów na sekundę) - największy wolumetryczny atak zaobserwowany w sieci Orange Polska



prawdopodobne zagrożenia 2015

- wzrost siły ataków DDoS
- zagrożenia dla platform mobilnych (Android)
- phishing - poczta i www
- ataki ATP na organizacje - wyszukaj i zniszcz
- kradzież danych osobowych
- ataki na Internet Rzeczy
- cyber-terroryzm, cyber-konflikty, cyber-szpiegostwo

Zespół CERT Orange Polska
to 18 lat doświadczeń

CERT

FIRST
Improving Security Together

ACCREDITED BY TI TRUSTED INTRODUCER

dziękuję