Rok 2025 wg CERT Orange Polska: AI zmienia krajobraz zagrożeń, dominują fałszywe inwestycje. Odporność ma wiele wymiarów

Informacja prasowa, 31 marca 2026

Blisko 70% wszystkich fałszywych stron jakie w ub. roku zablokował CERT Orange Polska dotyczyło fałszywych inwestycji. W sumie CyberTarcza Orange zablokowała rekordową liczbę 345 tys. domen phishingowych. Niemal 5,5 mln osób, próbujących wejść na zablokowane wcześniej strony, uniknęło utraty danych i pieniędzy. Ponad 40 tysięcy osób korzysta z rozwiązania Orange Hasło Alert by sprawdzać, czy ich dane logowania nie wyciekły do sieci. Firma udostępnia internautom nowe narzędzie do weryfikacji złośliwych domen.

- Budujemy nasze kompetencje w cyberbezpieczeństwie od wielu lat i choć zagrożeń przybywa lawinowo, w takim samym tempie rośnie nasza skuteczność w ich wykrywaniu i blokowaniu. Wykorzystujemy najnowsze technologie – sztuczną inteligencję i uczenie maszynowe. Krajobraz wyzwań jest dziś bardzo złożony. Mierzymy się z cyberatakami, gdzie również widać ogromny wpływ technologii, z ekstremalnymi zjawiskami klimatycznymi zakłócającymi łączność, zagrażają nam blackouty. Dlatego odporna sieć telekomunikacyjna w czasach, kiedy nasza codzienność tak mocno bazuje na rozwiązaniach cyfrowych, jest fundamentem bezpieczeństwa. Wzmacniamy ją na wiele sposobów - testujemy zabezpieczenia poprzez symulowane awarie, poprawiamy architekturę sieci, eliminujemy słabe punkty. Kluczowa jest także współpraca pomiędzy operatorami oraz z firmami z innych sektorów. Odporna sieć telekomunikacyjna, rozwiązania chroniące naszych klientów przed cyberzagrożeniami, a także świadomość nas wszystkich, nasza odporność na socjotechnikę – to wszystko składa się na bezpieczeństwo – powiedział Piotr Jaworski, członek zarządu Orange Polska ds. Sieci i Technologii.

Krajobraz cyberzagrożeń 2025 wg CERT Orange Polska

Jak wynika z najnowszego raportu CERT Orange Polska, główne kategorie ataków i ich udział wśród zagrożeń utrzymuje się od kilku lat na podobnym poziomie. Największą część stanowi **phishing - ponad 47% w roku 2025**, kolejne miejsca zajmują **ataki DDoS (niemal 16%) i złośliwe oprogramowanie (ponad 13%).** Charakter zagrożeń, sposób realizacji ataków zmienia się jednak diametralnie. Widać wpływ technologii, zwłaszcza AI oraz profesjonalizację przestępczego biznesu.
W kategorii phishingu - wyłudzania danych lub pieniędzy, **dominowały fałszywe inwestycje (niemal 70% wszystkich oszustw** vs zaledwie 28% dwa lata wcześniej). Coraz więcej fałszywych SMS-ów jest wysyłanych ze specjalnych aplikacji, to proceder zautomatyzowany, pozwalający działać na masową skalę.

- *Sztuczna inteligencja niestety mocno wspiera pomysłowość cyberprzestępców. Pomagają im także wielowarstwowe mechanizmy ukrywania oszustw i tworzenia fałszywych domen na masową skalę. Oszustwa na fałszywe inwestycje to kolejny etap rozwoju automatyzacji phishingu – tym początkowym były oszustwa na kupującego, gdzie domeny tworzono pod konkretnego użytkownika. W tym aspekcie dziś obserwujemy działania w pełni automatyczne i masowe* – powiedział Robert Grabowski, szef CERT Orange Polska.

DDOS – nowe rekordy, potężne botnety

Wśród ataków DDoS, największą część stanowią te krótkie, poniżej 10 minut, o niskim poziomie nasilenia, choć w ub. roku w sieci Orange zarejestrowano także ataki o rekordowej sile, sięgającej nawet 1,5 Tb/s. Rok 2025 przyniósł nowe, potężne, wielomilionowe botnety umożliwiające gigantyczne ataki jak np. Aisuru. Ataki przestają być jednorazowym zdarzeniem, a zaczynają wspierać inne działania, takie jak: kampanie dezinformacyjne, próby wymuszeń czy odwracanie uwagi od równolegle prowadzonych operacji. Platformizacja sprawia, że DDoS staje się łatwo dostępną usługą, możliwą do precyzyjnego zaplanowania, co fundamentalnie zmienia jego rolę w ekosystemie zagrożeń. Jak wskazują eksperci CERT Orange Polska, DDoS staje się zagadnieniem odporności architektury sieciowej jako całości. Skuteczna obrona wymaga dziś nie tylko dużych zasobów sieciowych, ale też m.in. ścisłej współpracy pomiędzy operatorami, CERT-ami i globalnymi dostawcami usług bezpieczeństwa.

Trendy w cyberbezpieczeństwie wg CERT Orange Polska

Nowe trendy widać także w atakach z użyciem złośliwego oprogramowania – atakujący coraz częściej wykorzystują asystentów AI, by zwiększyć skuteczność czy przekształcić dotychczasowe techniki na potrzeby ataków masowych. AI zmienia cyberbezpieczeństwo we wszystkich wymiarach – technologicznym, organizacyjnym i społecznym, stając się równocześnie narzędziem wspierającym obronę i ulepszającym działania zespołów cyberbezpieczeństwa.

Eksperci wskazują najpilniejsze wyzwania: podatności w urządzeniach sieciowych, coraz bardziej złożone działania grup APT (Advanced Persistent Threat) oraz rosnącą skalę kampanii celowanych. Aktywne podejmowanie działań ochronnych, ciągły „threat hunting”, systematyczne przygotowywanie scenariuszy reakcji nie są już działaniami „na wszelki wypadek”, lecz koniecznością.

Chroń swoją cyfrową tożsamość – nowe narzędzie od Orange

Ponad 40 tys. internautów korzysta już z bezpłatnej funkcjonalności **Hasło Alert**, dostępnej na stronie cert.orange.pl oraz w aplikacji Mój Orange. Dzięki niej można sprawdzić, czy dane logowania nie wyciekły do sieci. Narzędzie przeszukuje ogromne bazy wycieków danych, liczące miliardy rekordów. Jeśli nasze dane się w nich pojawiają, należy jak najszybciej zmienić hasło, a tam gdzie to możliwe, włączyć dwuskładnikowe uwierzytelnianie.

Orange Polska udostępnił właśnie **nowe narzędzie**, dzięki któremu użytkownicy mogą **sprawdzić, czy strona, na którą chcą wejść jest fałszywa i zablokowana w sieci Orange.**

- *Tego typu rozwiązania wzmacniają społeczną cyberodporność. Cieszy nas ogromna pomoc jaką otrzymujemy od internautów - każdy, kto wysłał do nas informację o zagrożeniach przyczynia się do naszego wspólnego bezpieczeństwa w sieci. To właśnie nasza świadomość i aktywność pozostaje kluczowym elementem ochrony cyfrowej tożsamości* – przekonuje Robert Grabowski.

W stronę cyberodporności biznesu

Orange konsekwentnie odpowiada na potrzeby firm w dziedzinie cyberbezpieczeństwa. Rok 2025 przyniósł dużą liczbę incydentów dotykających technologie operacyjne (OT) w infrastrukturze krytycznej i przemysłowej. Przeglądy bezpieczeństwa, wskazanie obszarów do poprawy, zrozumienie ryzyk związanych z lukami w zabezpieczeniach i zdefiniowanie planu naprawczego to pierwsze kroki na drodze ku firmowej cyberodporności.

- *W budowaniu świadomości zagrożeń i sposobów ochrony nic nie działa tak dobrze jak praktyka. W tym celu powstało nasze Laboratorium OT, gdzie pokazujemy przykłady ataków na infrastrukturę przemysłową i działanie narzędzi bezpieczeństwa. To także bezpieczne środowisko z rzeczywistymi, fizycznymi elementami automatyki i SCADA, które pozwala testować różne rozwiązania* – mówi Krzysztof Bronarski z zespołu ICT Orange Polska.

Podobnie jak w przypadku indywidualnych użytkowników, również w firmach najważniejszym punktem w systemie bezpieczeństwa są ludzie – ich świadomość i odporność na socjotechnikę. Oprócz **Centrum Doświadczeń Cyberbezpieczeństwa**, w którym uczymy jak lepiej chronić swoją firmę przed cyberatakami, także **Cyber Pakiet**, wspiera budowanie świadomości. Prócz rozwiązań takich jak np. skanowanie podatności infrastruktury klienta, ochrona reputacji firmy czy informacji na temat wycieków danych klienta, oferuje testy socjotechniczne, czyli uzgodnione, symulowane ataki phishingowe. Firmy chętnie korzystają także z **CyberWatcha**, ze względu na ochronę przed podstawowymi zagrożeniami, prostą i przyjazną obsługę. Klient otrzymuje m.in. szczegółowe informacje ilu użytkowników, z jakich adresów IP lub służbowych numerów, mogło połączyć się ze szkodliwą stroną. Sporym zainteresowaniem cieszy się też **ochrona przed atakami DDoS**.

Źródło: blog Orange Polska https://biuroprasowe.orange.pl