# Czym jest raport ekspozycji Atende Attack Surface 360°?

Wynikiem usługi Atende Attack Surface 360° jest raport ekspozycji cybernetycznej organizacji, budowany w oparciu o rzeczywiste dane techniczne z procesu skanowania infrastruktury oraz analizę zewnętrznych źródeł informacji o zagrożeniach. Nie jest to dokument deklaratywny ani checklistowy – to operacyjny snapshot ryzyka, pokazujący jak firma wygląda „z perspektywy Internetu" w danym momencie czasu.

Zakres raportu obejmuje pełną identyfikację i ocenę powierzchni ataku organizacji. Raport zaczyna się od jasno zdefiniowanego zakresu domen, subdomen i hostów, które wchodzą w skład infrastruktury firmy – zarówno środowisk produkcyjnych, jak i testowych, stagingowych czy zapomnianych zasobów, które często bywają największym problemem. Zakres ten nie jest ręcznie wpisywany, tylko dynamicznie budowany na podstawie danych wejściowych i automatycznego wykrywania, co eliminuje ryzyko „ślepych plam".

W kolejnej części raport prezentuje wyniki skanowania podatności i konfiguracji, agregując dane z kilku klas narzędzi: wykrywania usług sieciowych, identyfikacji systemów operacyjnych, analizy konfiguracji TLS/SSL, nagłówków bezpieczeństwa HTTP oraz testów aplikacyjnych. Kluczowe jest to, że raport nie skupia się wyłącznie na CVE, ale pokazuje również słabe konfiguracje, które same w sobie nie są podatnością krytyczną, ale realnie obniżają poziom bezpieczeństwa i zwiększają powierzchnię ataku. Z perspektywy biznesu to bardzo istotne, bo większość realnych incydentów zaczyna się właśnie od takich „niskich" problemów.

Raport zawiera także skondensowaną analizę wyników skanów aplikacyjnych, w której identyfikowane są powtarzalne klasy problemów, ich częstotliwość oraz potencjalny wpływ biznesowy. Zamiast setek surowych logów, odbiorca dostaje syntetyczne podsumowanie: co się powtarza, gdzie, jak często i dlaczego to ma znaczenie. To umożliwia podejmowanie decyzji priorytetyzacyjnych bez wchodzenia w techniczne detale.

Istotnym wyróżnikiem raportu jest sekcja dotycząca wycieków danych (Breaches Report). Raport koreluje skanowane domeny z danymi pochodzącymi z historycznych wycieków informacji, pokazując, czy konta, adresy e-mail, hasła lub URL-e powiązane z organizacją pojawiły się w znanych incydentach. Z biznesowego punktu widzenia jest to most pomiędzy bezpieczeństwem infrastruktury a ryzykiem tożsamościowym, reputacyjnym i prawnym. Raport nie tylko mówi „co jest źle skonfigurowane", ale również „jakie dane firmy już krążą poza jej kontrolą".

Uzupełnieniem analizy podatności i wycieków danych jest sekcja Phishing Domain Scanner, która koncentruje się na ryzyku podszywania się pod markę organizacji. W tej części raport identyfikuje domeny łudząco podobne do domen firmowych, powstałe w wyniku literówek, zamian znaków, alternatywnych rozszerzeń czy celowych manipulacji nazwą. Analiza nie ogranicza się do teoretycznych permutacji – raport wskazuje domeny realnie zarejestrowane i aktywne w DNS, a więc takie, które mogą być faktycznie wykorzystane w kampaniach phishingowych, atakach typu brand abuse lub do dystrybucji złośliwego oprogramowania.

Z perspektywy biznesowej ta część raportu przesuwa ciężar bezpieczeństwa z infrastruktury na ochronę marki, klientów i pracowników.

Raport pokazuje, gdzie istnieje realne ryzyko podszycia się pod organizację w komunikacji e-mailowej, na fałszywych portalach logowania czy w kampaniach socjotechnicznych. Dzięki temu firma zyskuje możliwość wczesnej reakcji – zanim dojdzie do incydentu reputacyjnego, wyłudzeń finansowych lub utraty zaufania klientów.

Phishing Domain Scanner wzmacnia również współpracę między bezpieczeństwem prawnym i marketingiem. Dane z raportu mogą być bezpośrednio wykorzystane do decyzji o przejęciu domen, uruchomieniu procedur takedown, zgłoszeń do rejestrów domen czy dostawców usług, a także do działań komunikacyjnych i podnoszenia świadomości użytkowników. W efekcie organizacja nie tylko reaguje na phishing, ale aktywnie ogranicza przestrzeń działania dla atakujących, zanim zagrożenie stanie się widoczne na poziomie operacyjnym lub medialnym.

Całość raportu jest przedstawiana w formacie PDF, gotowym do dystrybucji, archiwizacji i audytu. Raport zawiera znaczniki czasu, jednoznaczne odniesienie do zakresu oraz spójną strukturę, co sprawia, że może być traktowany jako dowód należytej staranności – zarówno wewnętrznie, jak i wobec regulatorów, audytorów czy partnerów biznesowych.

Jeśli chodzi o korzyści biznesowe, ten raport przede wszystkim skraca dystans między IT a zarządem. Zamiast ogólników typu „mamy dużo podatności", organizacja dostaje mierzalny obraz ryzyka, który można śledzić w czasie. Raport umożliwia porównywanie kolejnych iteracji, ocenę skuteczności działań naprawczych oraz realne zarządzanie ryzykiem, a nie tylko reagowanie na incydenty.

Druga kluczowa korzyść to optymalizacja kosztów bezpieczeństwa. Dzięki priorytetyzacji problemów i pokazaniu, które obszary faktycznie generują ryzyko, firma przestaje inwestować „na ślepo". Raport wspiera decyzje, gdzie warto wzmacniać zabezpieczenia, a gdzie ryzyko jest akceptowalne z punktu widzenia biznesu.

Raport jest skierowany do kilku grup odbiorców jednocześnie. Dla zespołów bezpieczeństwa i IT jest narzędziem operacyjnym, wskazującym konkretne obszary do poprawy. Dla kadry menedżerskiej i zarządu jest syntetycznym raportem ryzyka, który można omówić na poziomie decyzji, a nie konfiguracji serwerów. Dla działów compliance i risk management stanowi materiał dowodowy pokazujący ciągły nadzór nad bezpieczeństwem organizacji.

W szerszej perspektywie taki raport realnie wzmacnia firmę jako organizację odporną cyfrowo. Zmienia bezpieczeństwo z kosztu reaktywnego w proces zarządczy oparty na danych. Buduje dojrzałość organizacyjną, zwiększa przewidywalność ryzyka i ogranicza element zaskoczenia. W świecie, w którym incydenty są kwestią „kiedy", a nie „czy", ten raport przesuwa firmę z pozycji ofiary do pozycji podmiotu świadomie zarządzającego swoją ekspozycją.

To nie jest raport „do szuflady".
To narzędzie decyzyjne. I dokładnie w tej roli ma największą wartość biznesową.

Karol Kij
**Ekspert ds. cyberbezpieczeństwa w Atende S.A.**