PIERWSZY KONTAKT

Podpisanie umowy o zachowaniu poufności (NDA)

↓

Przedstawiciel managera sprzedaży i cyberbezpieczeństwa w Onwelo kontaktuje się z klientem w sprawie przyjętego w firmie podejścia i doświadczenia w zakresie testów penetracyjnych infrastruktury i aplikacji webowych.

Zanim nastąpi wymiana jakichkolwiek danych wrażliwych między firmą Onwelo a klientem, jeszcze na etapie wstępnych ustaleń należy podpisać umowę o zachowaniu poufności (NDA).

OCENA ZAKRESU PRAC

Wymogi projektu

Zakres testów

Scenariusze testowe

↓

W oparciu o wiedzę i dane przekazane przez klienta Onwelo opracowuje harmonogram testów penetracyjnych, ustala ich cele i przygotowuje scenariusze testowe w zgodzie z wymogami i oczekiwaniami zleceniodawcy.

W oparciu o uzgodniony zakres prac i inne ustalenia Onwelo przystępuje do realizacji projektu. Na tym etapie klient udostępnia niezbędne informacje, takie jak dane uwierzytelniania, środowisko testowe itp.

USTALENIA KONTRAKTOWE

Zakres prac

Start projektu

↓

Po zatwierdzeniu celów, harmonogramu i kosztorysu prowadzone są ustalenia kontraktowe i następuje oficjalny start projektu.

Ustalenia na tym etapie pozwalają nam określić oczekiwania klienta, przygotować scenariusze testowe i wybrać najlepszy model (white box, grey box lub black box).

TESTY

Testowanie

Sprawozdawczość

↓

W zależności od wybranego modelu (white box / grey box / black box) zespół Onwelo przeprowadza odpowiednie testy wybranego zakresu aplikacji lub systemów i dokonuje diagnozy podatności na zagrożenia.

Na etapie testów Onwelo pozostaje w stałym kontakcie z wyznaczonymi pracownikami po stronie klienta. Pozwala to na szybką reakcję w przypadku wykrycia w zakresie testowanej infrastruktury krytycznych podatności na zagrożenia, które mogą mieć wpływ na działalność biznesową klienta.

PONOWNE TESTY

Weryfikacja wcześniejszych wyników

Testowanie

Sprawozdawczość

↓

Po upływie terminu rozwiązania zdiagnozowanych problemów zespół Onwelo przeprowadza ponowne testy w wybranym zakresie. Sprawdzamy też aktualny stan aplikacji lub systemu, jeżeli wykryte zostaną nowe luki lub podatności na zagrożenia.

Ponowne testy nie mają na celu jedynie weryfikacji wcześniejszych wyników. Wszelkie zmiany wprowadzone w okresie między pierwszym a ponownym testem mogą stwarzać ryzyko powstania nowych luk bezpieczeństwa i podatności na zagrożenia. Może to mieć związek z naprawami, aktualizacjami, nowymi wersjami aplikacji, itp. Zespół Onwelo dokonuje na tym etapie oceny takiego ryzyka.

PODSUMOWANIE

Prezentacja sprawozdania

Omówienie wyników

Omówienie rekomendacji

Na żądanie klienta przygotowujemy osobne wersje sprawozdania. Jedno jest przeznaczone dla zarządu i przedstawia wyniki na poziomie biznesowym. Drugie, o charakterze bardziej technicznym, trafia do zespołów informatycznych i zespołu rozwoju oprogramowania; zawiera wszystkie dane i rekomendacje niezbędne do podniesienia poziomu bezpieczeństwa wybranego zakresu infrastruktury.

Najważniejszą korzyścią każdego testu penetracyjnego jest pogłębione zrozumienie problemu, co pozwala na minimalizację lub całkowite usunięcie danego ryzyka w przyszłości. Po zakończeniu audytu Onwelo przedstawia złożone sprawozdanie z podsumowaniem przygotowanym specjalnie dla wybranych odbiorców po stronie klienta (zarząd, właściciele przedsiębiorstwa, zespoły techniczne itp.). W cytowanych sprawozdaniach zespół Cyber Security Onwelo przedstawia wyniki audytu, weryfikację koncepcji (PoC) oraz dalsze rekomendacje.