

Regulamin nieodpłatnej usługi „Raport Bezpieczeństwa”

§ 1

Postanowienia ogólne

1. Niniejszy regulamin (zwany dalej „Regulaminem”) określa zasady świadczenia nieodpłatnej usługi automatycznej, zdalnej weryfikacji poziomu bezpieczeństwa infrastruktury sieciowej (zwanej dalej „Usługą”) przez firmę EXEA Sp. z o.o. z siedzibą w Toruniu (zwaną dalej „Usługodawcą”).

2. Usługa ma charakter wyłącznie informacyjny, poglądowy oraz marketingowy. Jej celem jest identyfikacja i wskazanie potencjalnych podatności oraz błędów konfiguracyjnych weryfikowanej organizacji, widocznych od strony sieci Internet.

§ 2. Warunki korzystania i autoryzacja

1. Zleceniodawcą Usługi (zwanym dalej „Użytkownikiem”) może być wyłącznie podmiot gospodarczy posiadający pełne prawo i tytuł prawny do zarządzania oraz testowania infrastruktury teleinformatycznej powiązanej ze zgłaszaną domeną internetową.

2. Warunkiem uruchomienia Usługi jest:

- a) poprawne wypełnienie formularza (podanie adresu e-mail oraz nazwy domeny),
- b) złożenie oświadczenia o posiadaniu uprawnień do reprezentowania właściciela domeny i wyrażenie zgody na przeprowadzenie automatycznych testów bezpieczeństwa.
- c) potwierdzenie chęci wykonania Usługi poprzez kliknięcie w link aktywacyjny wystany na podany w formularzu adres e-mail.

3. Adres e-mail podany w formularzu musi znajdować się w domenie, która jest zgłaszana do weryfikacji (np. dla domeny `firma.pl` wymagany jest e-mail `nazwa@firma.pl`). Usługa nie zostanie uruchomiona do czasu pełnej weryfikacji dostępu do skrzynki odbiorczej.

§ 3. Zakres i metodologia działania narzędzia

1. Po poprawnej autoryzacji, o której mowa w § 2, dedykowane narzędzie Usługodawcy rozpocznie w pełni automatyczne działania testowe wobec zgłoszonej domeny oraz powiązanej z nią infrastruktury sieciowej.

2. W ramach Usługi narzędzie wykonuje następujące operacje automatyczne:

- a) enumerację (wykrywanie) subdomen powiązanych z domeną główną;
- b) skanowanie otwartych portów sieciowych;
- c) wykrywanie technologii oraz wersji usług uruchomionych na zidentyfikowanych zasobach;
- d) detekcję znanych podatności (CVE) oraz błędów w konfiguracji zabezpieczeń;
- e) weryfikację publicznie dostępnych baz danych pod kątem historycznych wycieków danych powiązanych ze zgłoszoną domeną.

3. Automatyczne testy są wykonywane wyłącznie ze zdefiniowanych adresów IP Usługodawcy. Wykaz aktualnych adresów IP, z których realizowane jest skanowanie, zostanie przekazany Użytkownikowi w wiadomości e-mail potwierdzającej uruchomienie Usługi, w celu umożliwienia ich ewentualnej autoryzacji przez dział IT Użytkownika.

4. Działania narzędzia koncentrują się na analizie konfiguracji i nie obejmują prób przełamania zabezpieczeń (np. ataków brute-force, SQL injection, odmowy usługi DoS/DDoS), niszczenia danych ani modyfikacji parametrów systemów Użytkownika.

§ 4. Efekt usługi i wyłączenie odpowiedzialności

1. Efektem działania narzędzia jest wygenerowanie i przestanie na zweryfikowany adres e-mail raportu na temat stanu bezpieczeństwa organizacji wraz z ogólnymi rekomendacjami naprawczymi.
2. Usługa jest świadczona w stanie takim, w jakim się znajduje („as is”). Raport ma charakter wyłącznie opinii technicznej i nie zastępuje pełnego, certyfikowanego audytu bezpieczeństwa ani testów penetracyjnych.
3. Usługodawca nie gwarantuje, że automatyczne narzędzie wykryje 100% podatności lub błędów konfiguracyjnych w systemach Użytkownika.
4. Użytkownik przyjmuje do wiadomości, że w przypadku stosowania zewnętrznych systemów ochrony, filtrowania ruchu lub sieci CDN (np. Cloudflare, zapory WAF), wyniki automatycznego skanowania mogą być ograniczone lub niepełne, za co Usługodawca nie ponosi odpowiedzialności.
5. Użytkownik przyjmuje do wiadomości, że automatyczne działania testowe (w szczególności skanowanie portów) mogą zostać zarejestrowane przez systemy bezpieczeństwa Użytkownika (np. zapory ogniowe, systemy IDS/IPS) jako incydent bezpieczeństwa.
6. Usługodawca nie ponosi żadnej odpowiedzialności za ewentualne przestoje, zakłócenia w działaniu systemów Użytkownika, fałszywe alarmy bezpieczeństwa, ani za jakiegokolwiek szkody (w tym utracone korzyści) powstałe bezpośrednio lub pośrednio w wyniku działania automatycznego narzędzia lub wykorzystania informacji zawartych w raporcie.

§ 5. Ochrona danych osobowych (RODO)

1. Administratorem danych osobowych podanych w formularzu oraz zebranych w procesie automatycznej weryfikacji jest firma Exea Sp. z o.o. z siedzibą w Toruniu (kod pocztowy 87-100), przy ul. Włocławskiej 167, nr KRS 0000394866, NIP: 9562295531, REGON: 341137054.
2. Dane (adres e-mail, nazwa domeny, adresy IP powiązane z domeną, dane o wyciekach) przetwarzane są w celu realizacji nieodpłatnej Usługi (art. 6 ust. 1 lit. b RODO) oraz w celu marketingu bezpośredniego usług własnych Administratora (art. 6 ust. 1 lit. f RODO).
3. Informacje o zidentyfikowanych w raporcie wyciekach danych pracowników Użytkownika są przekazywane wyłącznie do wiadomości Użytkownika w celu minimalizacji jego ryzyka biznesowego. Usługodawca nie staje się administratorem tych danych w celach innych niż realizacja Usługi i sporządzenie raportu.

§ 6. Postanowienia końcowe

1. Usługodawca zastrzega sobie prawo do odmowy wykonania Usługi lub przerwania automatycznego skanowania dla wybranej domeny bez podania przyczyny, w szczególności w przypadku podejrzenia nadużycia narzędzia.
2. W sprawach nieuregulowanych niniejszym Regulaminem zastosowanie mają odpowiednie przepisy prawa polskiego.