Ministerstwo Rozwoju i Technologii

plac Trzech Krzyży 3/5

00-507 Warszawa

Systematyzacja obszaru raportowania dostawców usług bezpieczeństwa WAF oraz łącz do Internetu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Data dd-mm-rrrr** | **Imię Nazwisko** | **Stanowisko** | **Podpis** |
| Przygotował | 09-02-2024 | Marcin Tynda | Certyfikowany audytor wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001 akredytowany przez Polskie Centrum Akredytacji nr rejestracyjny:  AC118-AWBI-20191122-R1-2293 |  |
| Sprawdził | 09-02-2024 | Maksym Brzęczek | Offensive Security Certified Professional |  |
| Zatwierdził | DD-MM-RRRR | Imię Nazwisko najwyższego z kierownictwa | Stanowisko |  |

**Informacje o zmianach w dokumencie**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Data**  **dd-mm-rrrr** | **Czynność zmiany** | **Miejsce zmiany dokumentu** |
| 1 | 02-02-2024 | d | Utworzenie dokumentu |
| 2 | 02-02-2024 | m | Modyfikacja wielu miejsc dokumentu |
| 3 | 04-02-2024 | m | Modyfikacja wielu miejsc dokumentu |
| 4 | 09-02-2024 | m | Modyfikacja wielu miejsc dokumentu |
| 9 | DD-MM-RRRR | z | Zatwierdzenie dokumentu |

Czynność zmiany – wartości: d- dodanie, m – modyfikacja, u- usunięcie, z-zatwierdzenie

**Spis treści**

[1. Business Impact Analysis 9](#_Toc160393149)

[19. Obowiązkowe dane w raporcie 11](#_Toc160393150)

[20. Informacja o zmianach po stronie dostawcy 12](#_Toc160393151)

[21. Analiza trendów główne zasady 12](#_Toc160393152)

[22. Graficzna wizualizacja 12](#_Toc160393153)

[22.1. Histogramy 12](#_Toc160393154)

[22.2. Wykresy kołowe 12](#_Toc160393155)

[22.3. Wykresy słupkowe 12](#_Toc160393156)

[22.4. Wykresy liniowe 13](#_Toc160393157)

[22.5. Mapy ciepła 13](#_Toc160393158)

[22.6. Wykresy punktowe (scatter plots): 13](#_Toc160393159)

[22.7. Wykresy Sankeya: 13](#_Toc160393160)

[23. Historia kontaktu/prób kontaktu 13](#_Toc160393161)

[24. Logi surowe (raw logs) 14](#_Toc160393162)

[25. Sposób dostarczenia raportu 14](#_Toc160393163)

[26. Czas pomiędzy raportami 14](#_Toc160393164)

[27. Elementy składowe raportu dla Web Application Firewall 14](#_Toc160393165)

[27.1. Najważniejsza informacja 14](#_Toc160393166)

[27.2. Struktura logu WAF 15](#_Toc160393167)

[27.2.1. Timestamp 15](#_Toc160393168)

[27.2.2. Adres IP Źródłowy 15](#_Toc160393169)

[27.2.3. Adres IP Docelowy 15](#_Toc160393170)

[27.2.4. Metoda Żądania HTTP 15](#_Toc160393171)

[27.2.5. URL Żądania 15](#_Toc160393172)

[27.2.6. User-Agent 15](#_Toc160393173)

[27.2.7. Kod Statusu Odpowiedzi HTTP 15](#_Toc160393174)

[27.2.8. Sygnatura Ataku/ID Reguły 15](#_Toc160393175)

[27.2.9. Akcja Podjęta przez WAF 16](#_Toc160393176)

[27.2.10. Payload/Body Żądania 16](#_Toc160393177)

[27.2.11. Referer 16](#_Toc160393178)

[27.2.12. Session ID 16](#_Toc160393179)

[27.2.13. Wartości Nagłówków Specyficznych dla Aplikacji 16](#_Toc160393180)

[27.3. Rodzaje ataków, które WAF powinien umieć blokować 16](#_Toc160393181)

[27.3.1. SQL Injection 16](#_Toc160393182)

[27.3.2. Cross-Site Scripting (XSS) 16](#_Toc160393183)

[27.3.3. Cross-Site Request Forgery (CSRF) 16](#_Toc160393184)

[27.3.4. Ataki typu DDoS 17](#_Toc160393185)

[27.3.5. Directory Traversal 18](#_Toc160393186)

[27.3.6. Remote File Inclusion (RFI) i Local File Inclusion (LFI) 18](#_Toc160393187)

[27.3.7. Ataki brute-force (siłowe) na mechanizmy autentykacji 18](#_Toc160393188)

[27.3.8. Command Injection 18](#_Toc160393189)

[27.3.9. XML External Entities (XXE) 18](#_Toc160393190)

[27.3.10. Ataki typu Path Traversal i Manipulacja Parametrami 18](#_Toc160393191)

[27.3.11. Retencja logów 18](#_Toc160393192)

[27.3.12. Zabezpieczenie logów 18](#_Toc160393193)

[27.3.13. Informacje statystyczne, trandy na podstawie przetworzonych logów 19](#_Toc160393194)

[27.4. Podsumowanie Wykrytych Zagrożeń 19](#_Toc160393195)

[27.5. Szczegóły Ataków 19](#_Toc160393196)

[27.6. Statystyki Ruchu Sieciowego 19](#_Toc160393197)

[27.7. Ocena Skuteczności Polityk Bezpieczeństwa 19](#_Toc160393198)

[27.8. Analiza Trendów 19](#_Toc160393199)

[27.9. Podatności i Rekomendacje 19](#_Toc160393200)

[27.10. Zdarzenia Bezpieczeństwa i Ich Rozwiązania 20](#_Toc160393201)

[27.11. Informacje o Konfiguracji WAF 20](#_Toc160393202)

[27.12. Użytkowanie Zasobów 20](#_Toc160393203)

[27.13. Feedback i Komentarze Użytkowników 20](#_Toc160393204)

[27.14. Załączniki 20](#_Toc160393205)

[27.14.1. Logi i Dane Techniczne 20](#_Toc160393206)

[27.14.2. Dokumentacja Techniczna 20](#_Toc160393207)

[28. Elementy składowe raportu dla analizy bezpieczeństwa ruchu w warstwach ISO/OSI o 3 do 6 21](#_Toc160393208)

[28.1. Struktura logu Firewall 21](#_Toc160393209)

[28.1.1. Timestamp (Znacznik czasu) 21](#_Toc160393210)

[28.1.2. Adres IP Źródłowy 21](#_Toc160393211)

[28.1.3. Port Źródłowy 21](#_Toc160393212)

[28.1.4. Adres IP Docelowy 21](#_Toc160393213)

[28.1.5. Port Docelowy 21](#_Toc160393214)

[28.1.6. Protokół 21](#_Toc160393215)

[28.1.7. Kierunek 21](#_Toc160393216)

[28.1.8. Akcja 21](#_Toc160393217)

[28.1.9. Rozmiar Pakietu 21](#_Toc160393218)

[28.1.10. ID Reguły 22](#_Toc160393219)

[28.1.11. Sygnatura Ataku/ID Zagrożenia 22](#_Toc160393220)

[28.1.12. Sesja 22](#_Toc160393221)

[28.1.13. Nagłówki Protokołu Warstwy Aplikacji: 22](#_Toc160393222)

[28.1.14. Informacje o autoryzacji/uwierzytelnieniu użytkowniku: 22](#_Toc160393223)

[28.1.15. Szczegóły Odpowiedzi 22](#_Toc160393224)

[28.2. Analiza Ruchu w Warstwie Sieciowej (Warstwa 3) 22](#_Toc160393225)

[28.3. Analiza Ruchu w Warstwie Transportowej (Warstwa 4) 22](#_Toc160393226)

[28.4. Analiza Ruchu w Warstwie Sesji (Warstwa 5) 22](#_Toc160393227)

[28.5. Analiza Ruchu w Warstwie Prezentacji (Warstwa 6) 23](#_Toc160393228)

[28.6. Analiza Specyficznych Ataków na Warstwy 3 do 6 23](#_Toc160393229)

[28.7. Rekomendacje Zabezpieczeń 23](#_Toc160393230)

[28.8. Podsumowanie Statystyk i Trendów 23](#_Toc160393231)

[28.9. Załączniki 23](#_Toc160393232)

[28.9.1. Szczegółowe Logi i Dane 23](#_Toc160393233)

[28.9.2. Dokumentacja Techniczna 23](#_Toc160393234)

Słownik

|  |  |  |
| --- | --- | --- |
| Lp | Definicja | Wyjaśnienie |
|  | BIA Business Impact Analysis | Analiza wpływu na biznes (BIA) jest kluczowym krokiem w procesie planowania ciągłości. BIA.  Celem BIA jest skorelowanie określonych komponentów IT z krytycznymi procesami, które obsługują i na podstawie tych informacji, w celu scharakteryzowania konsekwencji zakłócenia komponentów. Wyniki BIA powinny być odpowiednio uwzględnione w pracach związanych z analizą i opracowywaniem strategii dla planu odzyskiwania po awarii IT, planów naprawy biznesu i planu zarządzania incydentami [NIST 800-34].  Źródło: https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/bi-analysis |
|  | MRiT | Ministerstwo Rozwoju i Technologii Pl. Trzech Krzyży 3/5  00-507 Warszawa |
|  | Surowe logi (raw logs) | Nieprzetworzone logi w postaci wygenerowanej przez rozwiązanie, które te logi wytwarza. |
|  | Endpoint | Punkt końcowy np.: serwer, komputer, aplikacja w tym aplikacja webowa, URL w aplikacji webowej, który podlega monitorowaniu i powoduje wygenerowanie zapisu do logu. Może istnieć nieskończenie wiele endpointów. |
|  | Analiza trendów | To prezentacja interpretacji danych dotyczących aktywności i prób ataków na aplikacje internetowe, rejestrowanych przez WAF lub inne rozwiązanie. Celem tej analizy jest identyfikacja wzorców, tendencji i potencjalnych zagrożeń w czasie, aby umożliwić organizacjom lepsze zrozumienie obecnego krajobrazu zagrożeń i przewidywanie przyszłych ataków. Analiza trendów pomaga w optymalizacji konfiguracji, wzmocnieniu zabezpieczeń aplikacji webowych, a także w dostosowaniu polityk bezpieczeństwa do ewoluujących technik ataków i metod penetracji. |

# Business Impact Analysis

Zdecydowanie zalecamy przeprowadzanie analizy wpływu zdarzenia na organizację. Dzięki temu będzie możliwe wyskalowanie tych zdarzeń, które są krytyczne i na których należy się skupić.

Korzyści płynące z wykonania BIA dla podmiotów publicznych:

1. Zrozumienie krytyczności usług: BIA pomaga zidentyfikować, które usługi są najbardziej krytyczne dla funkcjonowania społeczeństwa i stabilności państwa. W sektorze publicznym, gdzie priorytetem jest dobro publiczne i bezpieczeństwo, zrozumienie, które usługi mają kluczowe znaczenie, jest niezbędne do planowania ciągłości działania i reagowania na kryzysy.
2. Ocena wpływu na społeczeństwo: Przeprowadzenie BIA pozwala ocenić, jak przerwanie dostępu do usług publicznych wpłynie na obywateli, np. przerwa w dostawie wody, awarie systemów zdrowotnych, czy zakłócenia w świadczeniu usług edukacyjnych. Dzięki temu możliwe jest priorytetyzowanie działań na rzecz minimalizacji negatywnego wpływu na społeczeństwo.
3. Zwiększenie odporności i gotowości na kryzysy: BIA w sektorze publicznym przyczynia się do lepszego przygotowania na różnorodne scenariusze, w tym katastrofy naturalne, ataki terrorystyczne, cyberataki czy pandemie. Poprzez identyfikację słabych punktów i planowanie reakcji, organy publiczne mogą zwiększyć swoją odporność i szybkość reagowania w sytuacjach kryzysowych.
4. Optymalizacja zasobów: W kontekście ograniczonych zasobów, BIA pomaga w efektywnym ich alokowaniu, zapewniając, że krytyczne usługi i procesy są odpowiednio wspierane, nawet w trudnych warunkach. Może to obejmować zarówno zasoby finansowe, ludzkie, jak i technologiczne.
5. Zgodność z przepisami i standardami: W wielu krajach przepisy wymagają od instytucji publicznych przeprowadzania regularnych analiz ryzyka i planowania ciągłości działania. BIA jest kluczowym elementem spełnienia tych wymagań, zapewniając zgodność z prawem i uniknięcie potencjalnych sankcji.

Przykład struktury analizy BIA

1. ID ryzyka: R005
2. Data identyfikacji ryzyka: 28.05.2022
3. Zasób dotknięty: Wiedza na temat zagrożeń bezpieczeństwa, problemów, luk jest nieaktualna.
4. Krótki opis ryzyka: Organizacja nie posiada aktualnej wiedzy na temat kwestii bezpieczeństwa informacji takich jak obecne zagrożenia, nowe kontrole i inne informacje.
5. Opis ryzyka: Wprowadź krótki opis ryzyka.
6. Surowa Wartość Aktywa (RAV): Wprowadź wartość. Surowa rzeczywista wartość samego aktywa bez uwzględnienia zawartych w nim informacji.
7. Wartość Informacji Aktywa (AIV): Wprowadź wartość. Wartość ta reprezentuje oszacowanie w walucie użyteczności, znaczenia, zakresu, użycia, wartości, wrażliwości i krytyczności informacji aktywa.
8. Dodatkowe wyjaśnienie: Wprowadź opis podstaw obliczania wartości.
9. Wartość Aktywa (AV): Całkowita wartość aktywa. Obliczana przez zsumowanie RAV i AIV. Koncepcja wartości w tym przypadku odzwierciedla wartość RAV i AIV.
10. Współczynnik Ekspozycji (EF): Wprowadź % wartości. Reprezentuje prawdopodobny procent aktywa, który zostanie utracony, jeśli zagrożenie się zmaterializuje.
11. Ekspozycja na Pojedynczą Stratę (SLE): Szacunkowa wartość straty dla aktywa związana z jednym wystąpieniem zagrożenia. Wartość wyrażona jest w walucie. W większości przypadków jest równa wartości aktywa, w tym uwzględnienia informacji, które znajdują się na aktywie. SLE jest obliczane przez pomnożenie AV i EF.
12. Roczna Częstotliwość Wystąpienia (ARO): Wprowadź ilość ryzyka, które ma zostać zminimalizowane w procentach.
13. Ekspozycja na Ryzyko (RE) / Roczne Oczekiwane Straty (ALE): Koszt ekspozycji na ryzyko jest obliczany przez pomnożenie SLE przez ARO. Ekspozycja na ryzyko jest innym sposobem odniesienia do Rocznych Oczekiwanych Strat (ALE). Jest to całkowity potencjalny koszt reaktywnego radzenia sobie ze wszystkimi wystąpieniami aktywa. Wartość wyrażona jest w walucie. Wartość jest obliczana.
14. Procent Zminimalizowanego Ryzyka (MRP): 99,9995%
15. Zminimalizowana Ekspozycja na Ryzyko (MRE): Jest to wartość w walucie, która nie będzie już zagrożona dzięki działaniom łagodzącym. Wartość ta jest obliczana przez pomnożenie RE przez MRP. Wartość wyrażona jest w walucie.
16. Pozostała Ekspozycja na Ryzyko (RRE): Jest to wartość w walucie oczekiwanej pozostałej (niezniwelowanej) ekspozycji na ryzyko i jest obliczana przez odjęcie MRE od RE.
17. Koszt Rozwiązania Leczącego (TSC): Wprowadź całkowity koszt leczenia (rozwiązania) na rok, który zmniejszy ekspozycję na ryzyko.
18. Zwrot z Inwestycji w Bezpieczeństwo (ROSI): Zwrot z inwestycji w bezpieczeństwo (ROSI) jest obliczany poprzez pomnożenie RRE przez MRP. TSC jest następnie odejmowany od tej wartości. Wynik jest następnie dzielony przez TSC. Końcowa wartość jest wyrażona w walucie.





# Obowiązkowe dane w raporcie

Ważną zasadą, którą należy stosować jest niepomijanie w raporcie informacji o atakach, które się nie wydarzyły. Nawet w sytuacji, gdy nie wystąpił atak DDoS należy napisać np.: Atak DDoS – nie stwierdzono itd.

Dzięki temu będzie możliwa weryfikacja poprzez jednoznacznie wskazanie stanu za wybrany okres oraz porównanie np.: z informacjami o degradacji usług.

# Informacja o zmianach po stronie dostawcy

O planowanych zmianach Dostawca winien informować z co najmniej sześciomiesięcznym wyprzedzeniem oraz o wpływie tych zmian na MRiT.

Dostawca usług bezpieczeństwa winien przynajmniej na miesiąc przed wprowadzanymi zmianami informować o tym klienta oraz o wpływie tych zmian na klienta.

# Analiza trendów główne zasady

Analiza trendów winna być dokonywana również na podstawie zanonimizowanego porównania zdarzeń występujących u klientów działających w tym samym sektorze gospodarki, posiadających podobną liczbę klientów, działających na podobną skalę – generalnie względem podobieństw.

# Graficzna wizualizacja

Prócz informacji tekstowych Dostawca winien obowiązkowo dostarczać informacje w postaci różnego rodzaju wykresów właściwych dla wizualizacji określonego rodzaju danych.

## Histogramy

* Idealne do prezentowania liczby ataków w określonym przedziale czasowym.
* Pozwalają na szybką ocenę wzrostu lub spadku aktywności ataków.
* Ułatwiają identyfikację wzorców ataków, takich jak godziny szczytu.

## Wykresy kołowe

* Skuteczne w pokazaniu procentowego rozkładu różnych typów ataków analizowanych przez WAF.
* Umożliwiają łatwe porównanie dominujących rodzajów ataków.
* Przydatne do podkreślenia najczęstszych zagrożeń.

## Wykresy słupkowe

* Doskonałe do porównywania liczby ataków między różnymi kategoriami, np. SQL Injection, XSS, DDoS.
* Pozwalają na wizualizację różnic w skali ataków pomiędzy poszczególnymi aplikacjami lub serwisami.
* Ułatwiają rozpoznawanie obszarów, które wymagają wzmocnienia zabezpieczeń.

## Wykresy liniowe

* Przydatne do pokazania trendów w czasie, np. jak zmieniała się liczba ataków dzień po dniu.
* Pozwalają na śledzenie dynamiki ataków i skuteczności wprowadzanych zabezpieczeń.
* Ułatwiają prognozowanie przyszłych wzorców ataków.

## Mapy ciepła

* Efektywne w pokazaniu intensywności ataków w zależności od lokalizacji geograficznej lub innych parametrów.
* Pomagają zidentyfikować regiony najbardziej narażone na ataki.
* Ułatwiają zrozumienie globalnego zasięgu zagrożeń.

## Wykresy punktowe (scatter plots):

* Idealne do analizy zależności między dwoma zmiennymi, np. czasem trwania ataku a jego skutecznością.
* Pozwalają na identyfikację nietypowych przypadków, które mogą wymagać dodatkowej analizy.
* Ułatwiają dostrzeżenie korelacji między różnymi rodzajami danych.

## Wykresy Sankeya:

* Skuteczne w wizualizacji przepływu danych między różnymi częściami aplikacji lub systemu, co może pomóc zrozumieć, jak ataki przenikają przez zabezpieczenia.
* Pozwalają na przedstawienie złożonych ścieżek ataków i interakcji między różnymi warstwami systemu.
* Ułatwiają identyfikację miejsc, w których ataki są blokowane lub przechodzą przez system.

# Historia kontaktu/prób kontaktu

W przypadku wystąpienia ataku Dostawca zobowiązany jest informować Klienta o tym fakcie najbardziej skuteczną oraz najszybszą drogą.

Wykonawca winien zachowywać historię podejmowanych prób kontaktu w postaci niezaprzeczalnej oraz rozliczanej np.: logi z systemu SMS, wirtualnej albo fizycznej centrali, logi sieci komórkowej.

# Logi surowe (raw logs)

MRiT powinien otrzymać jemu dedykowane logi źródłowe do ściągnięcia w każdej chwili nie rzadziej jednak niż raz dziennie. Przy dużej liczbie logów dostawca może je generować z opóźnieniem, ale raz na dobę najczęściej nie stanowi to problemu.

Logi powinny być udostępnione w postaci skompresowanego archiwum np.: tar.gz, zip inne podobne.

# Sposób dostarczenia raportu

Raport powinien być dostarczany w formie zaszyfrowanej o ile jest przesyłany pocztą elektroniczną. Ten sposób dystrybucji nie jest zalecany.

Automatycznie wygenerowany raportu winien być możliwy do ściągnięcia z dedykowanego zasobu Dostawcy po zalogowaniu się MRiT.

# Czas pomiędzy raportami

Raport winien być przekazywany co najmniej raz w tygodniu a w przypadku ataku przez kolejne 7 dni codziennie.

O ile to możliwe Dostawca powinien udostępnić raporty online i najlepiej czasie rzeczywistym klientowi aby ten mógł w każdej chwili sprawdzić stan.

# Elementy składowe raportu dla Web Application Firewall

## Najważniejsza informacja

W naszej ocenie najwięcej szkody przynoszą błędy występujące w warstwie 7 aplikacji. Tego rodzaju błędy mogą generować podatności typu Remote Code Execution.

W celu zapewnienia ochrony dla zasobów aplikacji dostawca usług WAF winien przed uruchomieniem usługi otrzymać informacje:

* o metodach użytych do autoryzacji użytkowników oraz sposobie wywołania tych metod w kodzie źródłowym,
* o endpointach aplikacji (endpoint to miejsce wywołania funkcji, metody, zwracania danych) które generują wysokie ryzyko np.:
  + miejsca autoryzacji użytkowników,
  + miejsca, których wywołanie uruchamia sktypty po stronie serwera,
  + miejsca, które odwołują się do systemu operacyjnego albo usług uruchomionych na serwerze, często powiązane z shell,
  + miejsca, w których wykonywane są płatności,
  + miejsca, w których przetwarzane są dane osobowe.
* Dla zasobów krytyczny mocno zalecane jest zapisywanie nie tylko HEADERS (nagłówków) requestów ale również BODY, w którym często znajdują się informacje niezbędne do prowadzenia analizy śledczej.

## Struktura logu WAF

Poniżej wskazano minimalną, zalecaną strukturę dla logu Web Application Firewall

### Timestamp

Data i czas w formacie YYYY-MM-DD hh:mm:ss wystąpienia zdarzenia, zazwyczaj w formacie UTC, co pozwala na precyzyjne śledzenie aktywności i identyfikację trendów.

### Adres IP Źródłowy

Adres IP klienta (użytkownika końcowego lub atakującego), który inicjuje żądanie, umożliwiając identyfikację potencjalnego źródła ataku.

### Adres IP Docelowy

Adres IP serwera docelowego, na który skierowane jest żądanie, co pozwala zrozumieć, który zasób był celem ataku.

### Metoda Żądania HTTP

Typ metody HTTP użytej w żądaniu (np. GET, POST, PUT), co daje wgląd w rodzaj akcji podjętej przez klienta.

### URL Żądania

Pełny adres URL żądanego zasobu, co pozwala na identyfikację celów ataków na konkretnych stronach lub aplikacjach.

### User-Agent

Informacja o przeglądarce lub kliencie używanym przez żądającego, co może pomóc w identyfikacji zautomatyzowanych narzędzi atakujących lub specyficznych klientów.

### Kod Statusu Odpowiedzi HTTP

Kod odpowiedzi serwera (np. 200, 404, 403), wskazujący, jak serwer zareagował na żądanie.

### Sygnatura Ataku/ID Reguły

Identyfikator reguły lub sygnatura ataku, która została wyzwalana, co pozwala na identyfikację rodzaju wykrytego zagrożenia.

### Akcja Podjęta przez WAF

Opis akcji podjętej przez WAF w odpowiedzi na żądanie (np. zablokowanie żądania, wyzwanie CAPTCHA, logowanie bez blokady).

### Payload/Body Żądania

Fragmenty danych wysłane w treści żądania, które mogą zawierać złośliwe dane wyzwalające alarmy WAF.

### Referer

Adres URL, z którego użytkownik został przekierowany, co może pomóc w śledzeniu ścieżek ataku.

### Session ID

Unikalny identyfikator sesji użytkownika, co umożliwia śledzenie aktywności użytkownika w czasie.

### Wartości Nagłówków Specyficznych dla Aplikacji

Wartości niestandardowych nagłówków HTTP, które mogą być używane przez aplikacje webowe i są istotne dla analizy.

## Rodzaje ataków, które WAF powinien umieć blokować

### SQL Injection

Ataki typu SQL Injection pozwalają atakującemu na manipulowanie zapytaniami SQL, co może prowadzić do nieautoryzowanego dostępu do danych. WAF analizuje ruch sieciowy w poszukiwaniu podejrzanych sekwencji znaków sugerujących próbę iniekcji SQL i blokuje takie żądania. Dzięki zastosowaniu zaawansowanych algorytmów, WAF jest w stanie skutecznie odróżnić legalne zapytania od złośliwych prób iniekcji.

### Cross-Site Scripting (XSS)

Cross-Site Scripting umożliwia atakującemu wstrzyknięcie złośliwego kodu JavaScript do stron widzianych przez użytkowników. WAF identyfikuje i blokuje żądania, które mogą być próbą wykonania skryptu XSS na stronie, chroniąc użytkowników przed kradzieżą danych czy przejęciem sesji. Ochrona przed XSS jest realizowana poprzez filtrowanie wejść aplikacji oraz analizę treści odpowiedzi.

### Cross-Site Request Forgery (CSRF)

CSRF polega na wykorzystaniu zaufanej sesji użytkownika do wykonania nieautoryzowanych działań na stronie internetowej. WAF wykorzystuje tokeny i polityki same-origin, aby zapobiegać nieautoryzowanym żądaniom pochodzącym z innych stron. Zapobiega to wykorzystaniu przez atakujących sesji użytkowników do przeprowadzania złośliwych działań.

### Ataki typu DDoS

#### Ataki wolumetryczne

Ataki wolumetryczne polegają na zasypywaniu serwera ogromną ilością ruchu, co przekracza jego przepustowość i uniemożliwia obsługę legalnych żądań. Najczęściej wykorzystują one technikę amplifikacji, gdzie atakujący wykorzystuje niewielką ilość własnego ruchu do generowania znacznie większego ruchu docelowego. Skutkiem jest zablokowanie dostępu do serwisów internetowych lub spowolnienie ich działania.

#### Ataki na Warstwę Aplikacji (Layer 7)

Ataki na warstwę aplikacji celują bezpośrednio w najbardziej wrażliwe punkty aplikacji internetowych, takie jak skrypty logowania, formularze wyszukiwania czy inne dynamicznie generowane strony. Przez nadmierne generowanie żądań do tych elementów, atakujący może spowodować przeciążenie serwera i uniemożliwić obsługę normalnego ruchu. Ataki te są trudniejsze do wykrycia i zablokowania, ponieważ ruch często wygląda jak legalne zapytania od użytkowników.

#### Ataki typu SYN Flood

Atak typu SYN Flood wykorzystuje mechanizm nawiązywania połączeń TCP, wysyłając do serwera wielokrotne żądania nawiązania połączenia (SYN), nie kończąc ich prawidłowo. Serwer, czekając na zakończenie każdego z tych połowicznych połączeń, alokuje na nie zasoby, co przy dużej liczbie fałszywych żądań może doprowadzić do wyczerpania dostępnych zasobów i uniemożliwienia obsługi nowych, legalnych połączeń.

#### Ataki UDP Flood

Ataki UDP Flood polegają na wysyłaniu dużej ilości pakietów UDP do losowych portów na serwerze docelowym. Ponieważ UDP jest protokołem bezpołączeniowym, serwer próbuje odpowiedzieć na każde zapytanie, co przy ogromnej liczbie fałszywych żądań może doprowadzić do przeciążenia serwera. Skutkiem jest znaczne spowolnienie działania serwisu lub całkowita utrata dostępności.

#### Ataki typu Ping of Death

Ataki typu Ping of Death wykorzystują pakiet ICMP (Internet Control Message Protocol) o rozmiarze przekraczającym maksymalny dozwolony (65,535 bajtów). Przesyłanie takich zmanipulowanych pakietów może spowodować przeciążenie lub zawieszenie systemu docelowego. Współczesne systemy są zazwyczaj odporne na tego typu ataki dzięki aktualizacjom bezpieczeństwa.

#### Ataki Slowloris

Ataki Slowloris mają na celu zablokowanie dostępu do serwera poprzez otwieranie wielu połączeń do serwera i utrzymywanie ich w stanie otwartym, wysyłając jedynie częściowe lub bardzo wolne zapytania. Dzięki temu serwer trzyma połączenia otwarte, czekając na zakończenie zapytania, co ostatecznie może doprowadzić do wyczerpania limitu połączeń i uniemożliwienia obsługi nowych użytkowników.

### Directory Traversal

Directory Traversal umożliwia atakującemu dostęp do plików i katalogów znajdujących się poza rootem serwera WWW. WAF wykrywa próby manipulowania ścieżkami w żądaniach HTTP, które mogłyby doprowadzić do nieautoryzowanego dostępu do systemowych plików. Blokuje żądania próbujące wykorzystać te podatności.

### Remote File Inclusion (RFI) i Local File Inclusion (LFI)

RFI i LFI to ataki polegające na wstrzyknięciu złośliwego kodu do aplikacji poprzez dołączenie plików z serwera lokalnego lub zdalnego. WAF skanuje żądania o potencjalne próby RFI/LFI, wykorzystując mechanizmy filtracji, aby zapobiegać wykonaniu złośliwego kodu na serwerze.

### Ataki brute-force (siłowe) na mechanizmy autentykacji

Ataki siłowe polegają na próbach zgadnięcia haseł poprzez systematyczne przetestowanie wielu kombinacji. WAF monitoruje próby logowania i może identyfikować oraz blokować zachowania sugerujące atak siłowy, np. poprzez ograniczenie liczby prób logowania z jednego adresu IP.

### Command Injection

Command Injection pozwala atakującemu na wykonanie dowolnych poleceń na serwerze aplikacji. WAF wykrywa próby wstrzyknięcia złośliwych poleceń do aplikacji i blokuje ruch sieciowy, który może zawierać złośliwe instrukcje.

### XML External Entities (XXE)

XXE umożliwia atakującym na przeprowadzenie ataków polegających na przetwarzaniu złośliwie skonstruowanych dokumentów XML. WAF identyfikuje i blokuje żądania zawierające referencje do zewnętrznych encji XML, zapobiegając wykorzystaniu tej podatności.

### Ataki typu Path Traversal i Manipulacja Parametrami

Path Traversal pozwala na dostęp do plików poza oczekiwanym katalogiem aplikacji. WAF wykrywa i blokuje próby manipulacji parametrami żądań HTTP, które mogą prowadzić do nieautoryzowanego dostępu do plików lub informacji.

### Retencja logów

Logi powinny być dostępne przez co najmniej 30 dni. Po tym czasie najstarsze dane powinny być napisane.

### Zabezpieczenie logów

W przypadku wykrycia ataków zakres logów, wygenerowanych podczas trwania ataku powinien zostać zabezpieczenie.

### Informacje statystyczne, trandy na podstawie przetworzonych logów

Informacje zwizualizowane w dashboard oraz przetworzone jako podstawa dla wizualizacji inny być zachowywane przez 5 lat od chwili ich przetworzenia. Jest to możliwe, ponieważ logi po przetworzeniu dostarczają skumulowanych informacji kilkadziesiąt razy mniej niż logów źródłowych.

## Podsumowanie Wykrytych Zagrożeń

Raport powinien zawierać zestawienie wykrytych zagrożeń w określonym okresie czasu. Dla każdego zagrożenia należy podać jego typ, datę wykrycia oraz krótki opis. Powinna być również dostępna informacja o liczbie prób ataku związanych z każdym zagrożeniem.

## Szczegóły Ataków

Dla każdego wykrytego ataku raport powinien dostarczać dokładne informacje, w tym źródło ataku (adres IP), docelowe zasoby systemu (np. konkretne URL-e) oraz metody ataku (inaczej rodzaje ataków). Ważne jest, aby raport zawierał także informacje o tym, czy atak został zablokowany przez WAF i w jakim czasie od wykrycia ataku WAF go zablokował, czy też doszło do jego przepuszczenia w całości czy w części.

## Statystyki Ruchu Sieciowego

Raport powinien przedstawiać analizę ruchu sieciowego przechwyconego i przefiltrowanego przez WAF. Należy uwzględnić wolumen ruchu, podział na ruch dozwolony i zablokowany, oraz najbardziej aktywne źródła ruchu.

## Ocena Skuteczności Polityk Bezpieczeństwa

Należy ocenić, jak skuteczne były zaimplementowane polityki bezpieczeństwa w zapobieganiu atakom. Raport powinien nawiązywać do opisywanych w dalszej części rekomendacji dotyczące modyfikacji polityk, aby zwiększyć poziom bezpieczeństwa aplikacji webowych.

## Analiza Trendów

Ważnym elementem raportu jest analiza trendów dotyczących ataków i zagrożeń w czasie. Umożliwia to identyfikację wzorców ataków i przewidywanie potencjalnych zagrożeń w przyszłości.

## Podatności i Rekomendacje

Raport powinien zawierać informacje o potencjalnych podatnościach wykrytych przez WAF. Dla każdej podatności powinny zostać zaproponowane rekomendacje dotyczące działań naprawczych lub zabezpieczających.

## Zdarzenia Bezpieczeństwa i Ich Rozwiązania

Powinien zawierać historię zdarzeń bezpieczeństwa, w tym informacje o tym, jak zostały rozwiązane. Kluczowe jest przedstawienie czasu reakcji na incydent oraz podjętych kroków naprawczych.

## Informacje o Konfiguracji WAF

Raport musi zawierać przegląd aktualnej konfiguracji WAF, wskazując na wszelkie zmiany dokonane w okresie sprawozdawczym. Powinien także ocenić wpływ tych zmian na poziom bezpieczeństwa.

## Użytkowanie Zasobów

Analiza wykorzystania zasobów przez WAF, w tym obciążenie procesora, zużycie pamięci i przepustowość sieci, jest ważna dla oceny wydajności i stabilności systemu.

## Feedback i Komentarze Użytkowników

Raport powinien zawierać sekcję z opiniami i komentarzami użytkowników dotyczącymi działania WAF, co może pomóc w identyfikacji obszarów wymagających poprawy.

## Załączniki

### Logi i Dane Techniczne

Powinna zawierać szczegółowe logi i dane techniczne dotyczące monitorowania i ataków, które mogą być użyte do głębszej analizy i lepszego zrozumienia zagrożeń.

### Dokumentacja Techniczna

Powinna zawierać linki do dokumentacji technicznej i zaleceń bezpieczeństwa, które mogą wspomóc organizację w implementacji najlepszych praktyk i zabezpieczeń.

# Elementy składowe raportu dla analizy bezpieczeństwa ruchu w warstwach ISO/OSI o 3 do 6

## Struktura logu Firewall

Poniżej wskazano minimalną, zalecaną strukturę dla logu Firewall

### Timestamp (Znacznik czasu)

Data i godzina zarejestrowania zdarzenia, zazwyczaj w formacie UTC, umożliwiająca precyzyjną analizę sekwencji zdarzeń.

### Adres IP Źródłowy

Adres IP urządzenia inicjującego połączenie, kluczowy do identyfikacji źródła ruchu sieciowego.

### Port Źródłowy

Numer portu źródłowego używanego przez urządzenie inicjujące połączenie, pomagający w określeniu typu usługi lub aplikacji.

### Adres IP Docelowy

Adres IP urządzenia docelowego, do którego kierowane jest połączenie, wskazujący na potencjalny cel ataku lub docelową usługę.

### Port Docelowy

Numer portu docelowego, który może wskazywać na konkretną usługę sieciową lub aplikację na urządzeniu docelowym.

### Protokół

Protokół wykorzystany do transmisji (np. TCP, UDP, ICMP), kluczowy do rozróżnienia rodzaju ruchu sieciowego.

### Kierunek

Kierunek ruchu (przychodzący/wychodzący), umożliwiający zrozumienie czy ruch był inicjowany z wewnątrz czy z zewnątrz sieci.

### Akcja

Działanie podjęte przez firewall w odpowiedzi na zdarzenie (np. zezwolenie, blokada, odrzucenie), które jest kluczowe do oceny polityki bezpieczeństwa.

### Rozmiar Pakietu

Rozmiar pakietu danych związany z zarejestrowanym zdarzeniem, mogący dostarczyć informacji o charakterze transmisji.

### ID Reguły

Identyfikator reguły firewalla, która została wyzwolona przez zdarzenie, umożliwiający łatwe śledzenie i analizę polityk bezpieczeństwa.

### Sygnatura Ataku/ID Zagrożenia

Jeśli firewall posiada możliwości wykrywania zagrożeń, zapisywany jest identyfikator wykrytego zagrożenia lub sygnatura ataku, co pomaga w szybkiej identyfikacji i reakcji na ataki.

### Sesja

Unikalny identyfikator sesji, jeśli jest stosowany, umożliwiający śledzenie i analizowanie ciągłości ruchu między konkretnymi punktami końcowymi.

### Nagłówki Protokołu Warstwy Aplikacji:

Informacje z nagłówków dla protokołów warstwy aplikacji (np. HTTP, HTTPS), jeśli są analizowane, co może dostarczyć szczegółów o typie żądania, URL, metodach HTTP itd.

### Informacje o autoryzacji/uwierzytelnieniu użytkowniku:

Informacje o użytkowniku lub procesie autentykacji, jeśli ruch sieciowy jest powiązany z konkretnym użytkownikiem lub sesją autentykacji.

### Szczegóły Odpowiedzi

Informacje o odpowiedziach na żądania sieciowe, w tym kody statusu dla protokołów HTTP/HTTPS, które mogą wskazywać na wynik prób dostępu do zasobów sieciowych.

## Analiza Ruchu w Warstwie Sieciowej (Warstwa 3)

Raport powinien zawierać szczegółową analizę protokołów IP, w tym statystyki dotyczące rozmiarów pakietów i typów protokołów (np. ICMP, TCP, UDP). Należy zidentyfikować i opisać nietypowe wzorce ruchu, które mogą wskazywać na próby ataków, jak np. skanowanie portów lub ataki DDoS. Ważne jest także wskazanie źródeł ruchu, zarówno wewnętrznych, jak i zewnętrznych, oraz ocena ich potencjalnego zagrożenia dla bezpieczeństwa sieci.

## Analiza Ruchu w Warstwie Transportowej (Warstwa 4)

Element ten powinien zawierać analizę sesji TCP i UDP, w tym otwarte połączenia, próby nawiązania połączeń oraz niespodziewane zakończenia sesji. Ważne jest, aby zwrócić uwagę na niezwykłą aktywność, taką jak nieoczekiwana liczba prób połączeń do określonych portów, co może sygnalizować ataki typu SYN flood. Raport powinien również zawierać informacje o wykorzystaniu portów, identyfikując te, które są najczęściej używane lub atakowane.

## Analiza Ruchu w Warstwie Sesji (Warstwa 5)

Raport musi przedstawić informacje o zarządzaniu sesjami, w tym mechanizmach utrzymywania stanu sesji i autentykacji. Należy zwrócić uwagę na wszelkie anomalie w zarządzaniu sesjami, które mogą wskazywać na ataki, jak np. sesje trwające nietypowo długo lub mające nietypową aktywność. Powinien również oceniać zabezpieczenia przeciwko atakom polegającym na przejęciu sesji.

## Analiza Ruchu w Warstwie Prezentacji (Warstwa 6)

Ten element raportu powinien skupić się na sposobie kodowania danych, kompresji oraz szyfrowania, stosowanych w komunikacji między klientem a serwerem. Ważne jest, aby zidentyfikować i opisać wszelkie słabości w implementacji tych mechanizmów, które mogłyby zostać wykorzystane przez atakujących. Analiza powinna także obejmować ocenę używanych algorytmów szyfrowania i ich odporność na znane metody ataków.

## Analiza Specyficznych Ataków na Warstwy 3 do 6

Raport musi zawierać szczegółowy opis specyficznych ataków, które celują w warstwy 3 do 6 modelu OSI, wskazując, jakie techniki atakujący wykorzystali, jakie były ich cele i jakie środki obronne okazały się skuteczne. Należy w tym kontekście opisać zarówno próby ataków zidentyfikowane bezpośrednio w trakcie analizy, jak i potencjalne zagrożenia oparte na obserwacji nietypowych wzorców ruchu.

## Rekomendacje Zabezpieczeń

Na podstawie przeprowadzonej analizy, raport powinien zawierać zestaw rekomendacji mających na celu poprawę bezpieczeństwa sieci i aplikacji. Rekomendacje te powinny być konkretnymi propozycjami działań, takich jak zmiany konfiguracji, aktualizacje oprogramowania, wzmocnienie polityk bezpieczeństwa, które mogą pomóc w ochronie przed wykrytymi i potencjalnymi zagrożeniami.

## Podsumowanie Statystyk i Trendów

Ostatni element raportu powinien przedstawiać podsumowanie najważniejszych statystyk ruchu oraz analizę trendów w czasie. Powinien zawierać informacje o ogólnym wzroście lub spadku ruchu w analizowanych warstwach oraz jak zmieniały się rodzaje i skala ataków. To pozwala na lepsze zrozumienie ogólnej postawy bezpieczeństwa i identyfikację długoterminowych wzorców, które mogą wymagać uwagi.

## Załączniki

### Szczegółowe Logi i Dane

Dostarcza szczegółowych logów i danych technicznych, które były podstawą analizy, umożliwiając dokładniejsze dochodzenie w przypadku potrzeby.

### Dokumentacja Techniczna

Zapewnia dostęp do szczegółowej dokumentacji technicznej użytych narzędzi i standardów, co może pomóc w dalszym rozwoju strategii bezpieczeństwa.