Metodologia oceny ryzyka OWASP

Odkrywanie luk w zabezpieczeniach jest ważne, ale oszacowanie związanego z tym ryzyka dla firmy jest równie ważne. Na wczesnym etapie cyklu życia można zidentyfikować problemy związane z bezpieczeństwem w architekturze lub projekcie za pomocą modelowania zagrożeń. Później można znaleźć problemy bezpieczeństwa za pomocą przeglądu kodu lub testów penetracyjnych. Problemy mogą nie zostać wykryte, dopóki aplikacja nie zostanie uruchomiona lub zaatakowana.

Stosując opisane tutaj podejście, możliwe jest oszacowanie wagi wszystkich tych zagrożeń dla firmy i podjęcie świadomej decyzji o tym, co zrobić z tymi ryzykami. Posiadanie systemu umożliwiającego ocenę ryzyka pozwoli zaoszczędzić czas i wyeliminuje kłótnie o priorytety. System ten zapewni, że firma nie będzie rozproszona się przez niewielkie ryzyko, ignorując tym samym bardziej poważne zagrożenia, które są mniej zrozumiałe.

Idealnie byłoby, gdyby istniał uniwersalny system oceny ryzyka, który dokładnie oszacowałby wszystkie ryzyka dla wszystkich organizacji. Jednak luka krytyczna dla jednej organizacji może nie być ważna dla innej. Przedstawiono tutaj podstawowe ramy, które powinny być dostosowane do danej organizacji.

Autorzy starają się, aby ten model był prosty w użyciu, aby możliwe było dokładne oszacowanie ryzyka. Aby uzyskać więcej informacji o dostosowywaniu modelu do użytku w konkretnej organizacji, zapoznaj się z poniższą sekcją o dostosowywaniu.

Podejście
Istnieje wiele różnych podejść do analizy ryzyka. Podejście OWASP przedstawione tutaj opiera się na tych standardowych metodach i jest dostosowane do bezpieczeństwa aplikacji.

Zacznijmy od standardowego modelu ryzyka:

RYZYKO = PRAWDOPODOBIEŃSTWO * WPŁYW

W poniższych sekcjach czynniki, które składają się na "prawdopodobieństwo" i "wpływ" na bezpieczeństwo aplikacji, są rozbite. Tester pokazuje, jak je połączyć, aby określić ogólny poziom ryzyka.

Krok 1: Identyfikacja ryzyka
Pierwszym krokiem jest zidentyfikowanie zagrożenia, któremu należy nadać ocenę. Tester musi zebrać informacje o agencie ataku, o luce w zabezpieczeniach i wpływie skutecznego ataku na firmę. Może istnieć wiele możliwych grup atakujących lub nawet wiele możliwych wpływów biznesowych.

Krok 2: Czynniki szacowania prawdopodobieństwa
Po tym, jak tester zidentyfikuje potencjalne ryzyko i chce ustalić, jak jest poważne, pierwszym krokiem jest oszacowanie "prawdopodobieństwa". Jest to przybliżona miara prawdopodobieństwa, że luka zostanie odkryta i wykorzystana przez atakującego. W tym

oszacowaniu nie trzeba być zbyt precyzyjnym. Zasadniczo wystarczające jest stwierdzenie, czy prawdopodobieństwo jest niskie, średnie czy wysokie.

Istnieje szereg czynników, które mogą pomóc w ustaleniu prawdopodobieństwa. Pierwszy zestaw czynników jest związany z czynnikiem zagrożenia. Celem jest oszacowanie prawdopodobieństwa udanego ataku z grupy możliwych atakujących. Zauważ, że może istnieć wiele agentów niebezpieczeństwa, które mogą wykorzystać określoną lukę, więc najlepiej jest użyć najgorszego scenariusza. Na przykład ktoś z zewnątrz może być znacznie bardziej prawdopodobnym napastnikiem niż anonimowa osoba z zewnątrz, ale zależy to od wielu czynników.

Zauważ, że każdy czynnik ma zestaw opcji, a każda opcja ma przypisaną ocenę prawdopodobieństwa od 0 do 9. Liczby te zostaną wykorzystane później w celu oszacowania ogólnego prawdopodobieństwa.

Czynniki zagrożenia

Pierwszy zestaw czynników jest związany z agentami zagrożenia. Celem jest oszacowanie prawdopodobieństwa skutecznego ataku tej grupy agentów. Użyj najgorszego agenta.

- Poziom umiejętności

Jak technicznie wykwalifikowana jest ta grupa agentów? Umiejętności penetracji bezpieczeństwa (9), umiejętności sieciowe i programistyczne (6), zaawansowany użytkownik komputera (5), niektóre umiejętności techniczne (3), brak umiejętności technicznych (1)

- Motyw

Jak zmotywowana jest ta grupa agentów zagrożeń, aby znaleźć i wykorzystać tę lukę? Niska motywacja (1), średnia motywacja (4), wysoka motywacja (9)

- Możliwości

Jakie zasoby i możliwości są wymagane dla tej grupy agentów aby wykryć podatność i wykorzystać ją? Wymagany pełny dostęp lub kosztowne zasoby (0), specjalny dostęp lub wymagane zasoby (4), trochę wymaganego dostępu lub zasobów (7), nie wymagany dostęp lub zasoby (9)

- Rozmiar

Jak duża jest ta grupa agentów? Programiści (2), administratorzy systemu (2), użytkownicy intranetowi (4), partnerzy (5), uwierzytelnieni użytkownicy (6), anonimowi użytkownicy Internetu (9)

Czynniki podatności

Kolejny zestaw czynników jest związany z podatnościami. Celem jest oszacowanie prawdopodobieństwa, że dana podatność zostanie wykryta i wykorzystana. Załóżmy, że agent został wybrany powyżej.

- Łatwość wykrycia

Jak łatwo jest dla tej grupy agentów wykryć tę podatność? Praktycznie niemożliwe (1), trudne (3), łatwe (7), są dostępne narzędzia automatyczne (9)

- Łatwość wykorzystania

Jak łatwo jest dla tej grupy agentów wykorzystać tę podatność? Teoretycznie(1), trudno (3), łatwo (7), są dostępne narzędzia automatyczne (9)

- Świadomość

Jak dobrze znana jest ta luka w zabezpieczeniach tej grupie agentów? Nieznana (1), ukryta (4), oczywista (6), publicznie znana (9)

- Wykrywanie wtargnięcia

Jak prawdopodobne jest wykrycie wtargnięcia? Aktywne wykrywanie w aplikacji (1), logowanie i sprawdzanie (3), logowanie bez sprawdzania (8), niezalogowane (9)

Krok 3: Czynniki pozwalające oszacować wpływ

Rozważając wpływ udanego ataku, ważne jest, aby zdać sobie sprawę, że istnieją dwa rodzaje wpływów. Pierwszym jest "wpływ techniczny" na aplikację, wykorzystywane dane i funkcje, które zapewnia. Drugi to "wpływ na biznes" firmy i firmy obsługującej aplikację.

Ostatecznie wpływ na biznes jest ważniejszy. Użytkownik może jednak nie mieć dostępu do wszystkich informacji wymaganych do określenia biznesowych konsekwencji skutecznego ataku. W takim przypadku podanie jak największej liczby szczegółów na temat ryzyka technicznego umożliwi odpowiedniemu przedstawicielowi biznesowemu podjęcie decyzji o ryzyku biznesowym.

Ponownie, każdy czynnik ma zestaw opcji, a każda opcja ma ocenę wpływu od 0 do 9 z nim powiązaną. Wykorzystamy te liczby później, aby oszacować ogólny wpływ.

<u>Czynniki wpływu technicznego</u>

Wpływ techniczny można podzielić na czynniki odpowiadające tradycyjnym zagrożeniom bezpieczeństwa: poufność, integralność, dostępność i odpowiedzialność. Celem jest oszacowanie wielkości wpływu na system, jeśli luka zostanie wykorzystana.

- Utrata poufności

Ile danych może zostać ujawnionych i jak bardzo są wrażliwe? Minimalne niewrażliwe dane ujawnione (2), minimalnie krytyczne dane ujawnione (6), rozległe niewrażliwe dane ujawnione (6), rozległe dane krytyczne ujawnione (7), wszystkie dane ujawnione (9)

- Utrata integralności

Ile danych może być uszkodzonych i jak bardzo są uszkodzone? Minimalnie lekko uszkodzone dane (1), minimalnie poważnie uszkodzone dane (3), rozlegle lekko uszkodzone dane (5), rozlegle poważnie uszkodzone dane (7), wszystkie dane całkowicie uszkodzone (9)

- Utrata dostępności

Ile usług możesz stracić i jak bardzo jest to ważne? Przerwano minimalne usługi drugorzędne (1), przerwano minimalne usługi podstawowe (5), przerwano rozległe usługi drugorzędne (5), przerwano rozległe usługi podstawowe (7), wszystkie usługi całkowicie utracone (9)

- Utrata odpowiedzialności

Czy działania agentów zagrożeń są identyfikowalne dla danej osoby? W pełni identyfikowalne (1), możliwe do ustalenia (7), całkowicie anonimowe (9)

Czynniki wpływu na biznes

Wpływ na biznes wynika z wpływu technicznego, ale wymaga głębokiego zrozumienia tego, co jest ważne dla firmy, która prowadzi aplikację. Ogólnie rzecz biorąc, powinieneś starać się wspierać swoje ryzyko z wpływami biznesowymi, szczególnie jeśli twoja publiczność jest na poziomie wykonawczym. Ryzyko biznesowe uzasadnia inwestycje w rozwiązywanie problemów związanych z bezpieczeństwem.

Wiele firm ma przewodnik klasyfikacji aktywów i / lub odniesienie do wpływu na biznes, aby pomóc sformalizować to, co jest ważne dla ich działalności. Te standardy mogą pomóc Ci skoncentrować się na tym, co naprawdę ważne dla bezpieczeństwa. Jeśli nie są one dostępne, musisz porozmawiać z ludźmi, którzy rozumieją biznes, aby uzyskać ich opinię na temat tego, co jest ważne.

Poniższe czynniki są typowymi obszarami dla wielu firm, ale obszar ten jest jeszcze bardziej unikalny dla firmy niż czynniki związane z zagrożeniem, luką w zabezpieczeniach i wpływem technicznym.

- Straty finansowe

Ile szkód finansowych będzie wynikać z exploita? Mniej niż koszt naprawy luki (1), niewielki wpływ na roczny zysk (3), znaczący wpływ na roczny zysk (7), bankructwo (9)

- Obrażenia reputacyjne

Czy exploit może spowodować szkody reputacyjne, które mogłyby zaszkodzić firmie? Minimalne obrażenia (1), utrata głównych kontrahentów(4), utrata wartości firmy (5), uszkodzenie marki (9)

- Niezgodność

Jak bardzo brak zgodności naraża bezpieczeństwo? Drobne naruszenie (2), wyraźne naruszenie (5), naruszenie wysokiego szczebla (7)

- Naruszenie prywatności

Ile informacji umożliwiających identyfikację osoby można ujawnić? Jedna osoba (3), setki osób (5), tysiące ludzi (7), miliony ludzi (9)

Krok 4: Określenie stopnia zagrożenia
W tym kroku oszacowanie prawdopodobieństwa i oszacowanie wpływu są zestawione, aby obliczyć ogólną istotność dla tego ryzyka. Odbywa się to poprzez ustalenie, czy prawdopodobieństwo jest niskie, średnie lub wysokie, a następnie wykonanie tego samego dla wpływu. Skala od 0 do 9 podzielona jest na trzy części:

Prawdopodobieństwo i poziomy wpływu	
0 do < 3	NISKI
3 do < 6	ŚREDNI
6 do 9	WYSOKI

Nieformalna metoda
W wielu środowiskach nie ma nic złego w przeglądaniu czynników i po prostu przechwytywaniu odpowiedzi. Tester powinien przemyśleć wszystkie czynniki i zidentyfikować kluczowe czynniki "sterujące", które kontrolują wynik. Tester może odkryć, że początkowe wrażenie było błędne, biorąc pod uwagę aspekty ryzyka, które nie były oczywiste.

Powtarzalna metoda
Jeśli konieczne jest uzasadnienie ocen lub ich powtarzalność, należy przeprowadzić bardziej formalny proces oceny czynników i obliczenia wyniku. Należy pamiętać, że szacunki są dość niepewne i że te czynniki mają pomóc osobie testującej osiągnąć rozsądny wynik. Proces ten może być wspomagany przez automatyczne narzędzia, aby ułatwić obliczenia.

Pierwszym krokiem jest wybranie jednej z opcji powiązanych z każdym czynnikiem i wprowadzenie powiązanego numeru do tabeli. Następnie weź średnią wyników i oblicz ogólne prawdopodobieństwo. Na przykład:

Czynniki zagrożenia					Czynniki podatności			
Poziom umiejętności	Motyw	Możliwość	Wielkość		Łatwość wykrycia	Łatwość wykorzystania	Świadomość	Wykrywanie wtargnięć
5	2	7	1		3	6	9	2
Ogólne prawdopodobieństwo=4.375 (ŚREDNIE)								

Następnie tester musi ustalić ogólny wpływ. Proces jest podobny również tutaj. W wielu przypadkach odpowiedź będzie oczywista, ale tester może dokonać oszacowania na podstawie czynników lub może uśrednić wyniki dla każdego z czynników. Ponownie, mniej

niż 3 to niski wpływ, 3 do mniej niż 6 oznacza średni wpływ, a 6 do 9 to wysoki wpływ. Na przykład:

Wpływ techniczny					Wpływ na biznes			
Utrata poufności	Utrata integralności	Utrata dostępności	Utrata odpowiedzialności		Straty finansowe	Reputacja	Niezgodność	Naruszenie prywatności
9	7	5	8		1	2	1	5
Ogólne wpływ techniczny=7.25 (WYSOKI)					Ogólny wpływ biznesowy=2.25 (NISKI)			

<u>Określenie skali</u>

Jednak gdy tester dociera do oszacowań prawdopodobieństwa i wpływu, może je połączyć, aby uzyskać ostateczny wskaźnik skali dla tego ryzyka. Zwróć uwagę, że jeśli mają oni dobre informacje na temat wpływu na biznes, to powinni je wykorzystywać zamiast technicznych informacji o wpływie. Ale jeśli nie mają żadnych informacji na temat firmy, wpływ techniczny jest kolejną najlepszą rzeczą.

Ogólna skala ryzyka				
Wpływ	Wysoki	Średnie	Wysokie	Krytyczne
	Średni	Niskie	Średnie	Wysokie
	Niski	Nota	Niskie	Średnie
		Niskie	Średnie	Wysokie
	Prawdopodobieństwo			

W powyższym przykładzie prawdopodobieństwo jest średnie, a jego wpływ techniczny jest wysoki, więc z czysto technicznego punktu widzenia wydaje się, że ogólna skala jest wysoka. Należy jednak zauważyć, że wpływ na biznes jest w rzeczywistości niski, więc ogólną skalę najlepiej opisać jako niską. Dlatego zrozumienie kontekstu biznesowego analizowanych luk jest tak ważne dla podejmowania trafnych decyzji dotyczących ryzyka. Niezrozumienie tego kontekstu może prowadzić do braku zaufania między zespołem biznesowym a zespołem bezpieczeństwa, który jest obecny w wielu organizacjach.

Krok 5: Decydowanie co naprawić
Po sklasyfikowaniu ryzyka związanego z aplikacją zostanie ustalona priorytetowa lista tego, co należy naprawić. Ogólną zasadą jest, że najpoważniejsze zagrożenia należy naprawić w pierwszej kolejności. Naprawianie mniej istotnych zagrożenie nie wpływa pozytywnie na ogólny profil ryzyka, nawet jeśli zagrożenia te są łatwe lub tanie w naprawie.

Pamiętaj, że nie wszystkie ryzyka warto naprawiać, a niektóre straty są nie tylko spodziewane, ale uzasadnione w oparciu o koszt rozwiązania problemu. Na przykład, gdyby wdrożenie mechanizmów kontrolnych kosztowało 100 000 USD i miałoby na celu powstrzymać oszustwa w wysokości 2 000 USD rocznie, zwrot z tej inwestycji wymagałby 50 lat. Ale pamiętaj, że może dojść do zniszczenia reputacji z powodu oszustwa, które może kosztować organizację znacznie więcej.

Krok 6: Dostosowanie modelu oceny ryzyka
Posiadanie ram rankingu ryzyka, które można dostosować do potrzeb firmy, ma kluczowe znaczenie dla jego przyjęcia. Dopasowany model ma większe szanse na uzyskanie wyników, które pasują do spostrzeżeń ludzi na temat tego czym jest poważne ryzyko. Można zmarnować sporą ilość czasu na dyskusje o ocenie ryzyka jeśli nie jest ona wspierana przez taki modell. Istnieje kilka sposobów na dostosowanie tego modelu do organizacji.

- Dodawanie czynników

Tester może wybrać różne czynniki, które lepiej odzwierciedlają to, co jest ważne dla konkretnej organizacji. Na przykład aplikacja militarna może dodać czynniki wpływające na utratę życia ludzkiego lub informacje niejawne. Tester może również dodać czynniki wiarygodności, takie jak możliwość którą może wykorzystać atakujący lub siła algorytmu szyfrowania.

- Dostosowywanie opcji

Istnieje kilka przykładowych opcji związanych z każdym czynnikiem, ale model będzie znacznie bardziej efektywny, jeśli tester dostosuje te opcje do biznesu. Na przykład można użyć nazw różnych zespołów i nazw firm, aby uzyskać różne klasyfikacje informacji. Tester może również zmienić wyniki związane z opcjami. Najlepszym sposobem na określenie właściwych wyników jest porównanie ocen uzyskanych przez model z ocenami opracowanymi przez zespół ekspertów. Możesz dostosować model poprzez ostrożne dopasowanie wyników do siebie.

- Współczynniki wagowe

Powyższy model zakłada, że wszystkie czynniki są równie ważne. Możesz wyważyć czynniki, aby uwydatnić czynniki, które są bardziej istotne dla konkretnej firmy. To sprawia, że model jest nieco bardziej złożony, ponieważ tester musi stosować średnią ważoną. Ale w przeciwnym razie wszystko działa tak samo. Ponownie można dostosować model, dopasowując go do ocen ryzyka, które firma uważa za poprawne.