tenable

10 WSKAZAŃ I PRZECIWWSKAZAŃ

POMOCNYCH W TWORZENIU PROGRAMU ZARZĄDZANIA PODATNOŚCIAMI OPARTEGO NA RYZYKU

W tradycyjnych procesach zarządzania podatnościami liczba podatności jest często tak duża, że trudno nadążyć z ich usuwaniem – trudno również określić, które stanowią największe ryzyko dla organizacji.

Sytuacja komplikuje się jeszcze bardziej, jeśli polegasz wyłącznie na wynikach z systemu CVSS, decydując o tym, które obszary podatności usuwać jako pierwsze. Dzieje się tak dlatego, że wyniki CVSS nie uwzględniają faktycznego ryzyka, a tradycyjne procesy zarządzania podatnościami nie zapewniają kompleksowego wglądu we współczesne metody ataków.

W rezultacie powstają martwe pola, które mogą narazić Twoją organizację na ryzyko. Przejście z tradycyjnego procesu zarządzania podatnościami na program oparty na ryzyku może pomóc Ci nadawać podatnościom odpowiedni priorytet. Takie podejście zapewni Ci również lepszy wgląd we wszystkie zasoby narażone na atak, a także powiązane zagrożenia na powierzchni ataku.

Jeśli chcesz uzupełnić swój program zarządzania podatnościami o podejście oparte na ryzyku, rozważ poniższe wskazania i przeciwwskazania.

Wskazania	Przeciwwskazania
Tak Odkrywaj luki w swoich procesach zarządzania podatnościami, np. potencjalne martwe punkty, i sporządzaj plany naprawcze, aby poprawić ogólny stan zabezpieczeń.	**Nie** Nie zakładaj, że Twój program jest „wystarczająco dobry". Oceniaj dojrzałość programu bezpieczeństwa, aby upewnić się, że Twoje wskaźniki ryzyka są oparte na wysoce wiarygodnych danych.
Tak Identyfikuj i mapuj wszystkie swoje zasoby – nie tylko z tradycyjnego otoczenia IT, ale również ze środowiska mobilnego i chmurowego, OT, kontenerów i aplikacji internetowych.	**Nie** Nie koncentruj się wyłącznie na zasobach istotnych dla zachowania zgodności z przepisami. Dokonuj oceny wszystkich zasobów mających kluczowe znaczenie dla Twojej działalności.
Tak Zobacz wszystkie swoje zasoby i podatności w pełnym kontekście, aby koncentrować się na kluczowych kwestiach.	**Nie** Decydując o tym, które podatności usunąć jako pierwsze, nie polegaj wyłącznie na wynikach z systemu CVSS. Działania naprawcze należy priorytetyzować z uwzględnieniem pełnego kontekstu każdej podatności, w tym kluczowego znaczenia danych zasobów, oraz na podstawie oceny aktualnych i potencjalnych działań podejmowanych w ramach ataków.
Tak Stale oceniaj wszystkie znane zasoby oraz niezwłocznie identyfikuj i poddawaj ocenie nowe zasoby.	**Nie** Nie ograniczaj się do wyszukiwania i oceniania zasobów pod kątem podatności. Wybieraj bardziej kompleksowe rozwiązania. Priorytetyzuj każdą podatność w kontekście ryzyka biznesowego, podejmuj odpowiednie działania zaradcze oraz monitoruj kluczowe wskaźniki wydajności (KPI).
Tak Przyjmij aktywne, strategiczne podejście do zarządzania podatnościami, aby koncentrować uwagę na faktycznych zagrożeniach biznesowych, a nie na słabych punktach omawianych w mediach.	**Nie** Nie koncentruj uwagi wyłącznie na tradycyjnym środowisku IT oraz zasobach lokalnych. Identyfikuj i mapuj wszystkie swoje zasoby, również ze środowiska mobilnego, chmurowego, OT i kontenerów.
Tak Wykorzystuj uczenie maszynowe, aby automatycznie zestawiać dane o podatnościach i krytycznym znaczeniu zasobów z analizą zagrożeń i exploitów, co pozwala mierzyć i priorytetyzować podatności w kontekście ryzyka biznesowego.	**Nie** Nie próbuj ręcznie analizować dziesiątek tysięcy danych o zabezpieczeniach, aby ujrzeć podatności w szerszym kontekście. Wykorzystuj automatyzację uczenia maszynowego, aby szybko określać ryzyko biznesowe każdej podatności.
Tak W ciągu kolejnych 28 dni skoncentruj się na 3% podatności, które stwarzają największe ryzyko dla organizacji.	**Nie** Nie trać czasu na podatności, które nie stwarzają ryzyka. Skoncentruj się na podatnościach i zasobach, które są największym ryzykiem dla Twojej organizacji.
Tak Usuń podatności, które są największym ryzykiem dla organizacji.	**Nie** Nie opieraj decyzji o usuwaniu zagrożeń na przestarzałych, nieaktualnych informacjach z okazjonalnych skanów. Upewniaj się, że Twoja analiza zabezpieczeń jest tak samo dynamiczna, jak analiza zagrożeń.
Tak Używaj opartych na ryzyku wskaźników, aby ustalić poziom wydajności i skuteczności zespołu ds. zabezpieczeń.	**Nie** Nie mierz sukcesu liczbą usuniętych podatności ani wprowadzonych poprawek systemowych. Identyfikuj i naprawiaj zasoby oraz podatności, które stwarzają realne ryzyko dla Twojej organizacji. Usuwaj jak najwięcej zagrożeń przy minimalnym nakładzie pracy.
Tak Korzystaj z opartej na ryzyku analityki podatności oraz innych raportów badawczych, aby skuteczniej informować kluczowych interesariuszy o stanie zabezpieczeń – w przystępny sposób.	**Nie** Nie reaguj gorączkowo na każdą nową podatność, o której głośno w mediach. Podejście oparte na ryzyku pomoże Ci zwiększyć skuteczność i wydajność, dzięki czemu skoncentrujesz się na kluczowych kwestiach.

Chcesz ograniczyć ryzyko, zwiększyć skuteczność i skoncentrować się na kluczowych kwestiach? Tenable pomoże Ci włączyć podejście oparte na ryzyku do programu zarządzania podatnościami.

POZNAJ SZCZEGÓŁY