Arthur Braunstein
artykuł z dnia: 19.10. 2017

KLUCZOWE WSKAŹNIKI EFEKTYWNOŚCI (KPI)

Dwa kluczowe wskaźniki efektywności (KPI)

istotne w ocenie narzędzi bezpieczeństwa.

W zeszłym miesiącu omawiałem **skuteczność cyberbezpieczeństwa**, w szczególności w odniesieniu do rosnącego zagrożenia atakami bezplikowymi. Jednak skuteczność to tylko jeden element równania.

Przede wszystkim firmy nadal muszą zajmować się swoimi działaniami operacyjnymi. Niestety, jak dotychczas im bardziej skuteczne jest narzędzie zapewniające cyberbezpieczeństwo, tym jest ono wolniejsze i bardziej inwazyjne, a jego obsługa wymaga większego wysiłku.

Złożoność i utrapienie związane z zarządzaniem – nie kupowaniem, zarządzaniem! – narzędziami zapewniającymi bezpieczeństwo często sprawiają, że firmy godzą się na ryzyko nie do przyjęcia, na przykład na zakłócenia w działalności związane z bezpieczeństwem, z powodu braku zasobów do zarządzania nieefektywną technologią obronną.

Zabezpieczenia najlepiej wspierają biznes, kiedy są proste, nie wchodzą w drogę, nie odwracają uwagi od celów biznesowych lub nie zmuszają firmy do zmiany sposobu, w jaki ona działa.

Dwa kluczowe wskaźniki efektywności (KPI), szybkość i łatwość obsługi, są kluczowymi wskaźnikami dla jakiegokolwiek narzędzia zapewniającego bezpieczeństwo. Szybkość i łatwość obsługi oznaczają prostotę i łączą razem bezpieczeństwo, IT i biznes.

Szybki start

Czas nie jest sprzymierzeńcem cyberbezpieczeństwa. Jak tylko atak dotrze do punktu końcowego, uruchamia łańcuch wydarzeń, które podnoszą koszty i nakłady pracy włożone w bezpieczeństwo, IT, użytkowników końcowych i biznes. Dzieje się tak, ponieważ ataki są dynamiczne. Nie ustają, przeprowadzają rozpoznanie, zbierają informacje wywiadowcze, zmieniają się i namnażają i ostatecznie przygotowują się do wyprowadzenia danych lub unieruchomienia biznesu.

Wraz z postępującymi atakami, rośnie również wysiłek, jaki trzeba włożyć podczas stosowania narzędzi wykrywania, które monitorują, wykrywają, analizują i badają. Wysiłek ten zwiększa się na każdym etapie. To z jednej strony powoduje dodatkowe koszty, a z drugiej zwiększa prawdopodobieństwo zaniedbania, z powodu błędu ludzkiego. Na przykład, w wielu powtarzających się naruszeniach, wiedziano o ataku, ale pozwalano mu się rozwijać z powodu niewłaściwych decyzji związanych z oceną, niemożnością wyprzedzenia przebiegu ataku lub przeciążeniem związanym z zarządzaniem danym przypadkiem.

Nikt nie może traktować każdego alertu jako priorytet numer jeden, więc wiedza specjalistyczna i szczęście stają się cienką czerwoną linią pomiędzy sukcesem, a naruszeniem. Jeśli jednak zapobiegniemy atakowi w zaplanowany wcześniej sposób, zanim przeniknie, trud związany z wykryciem go i naprawieniem go spada w zasadzie do zera. Podobnie spadnie ryzyko, że atak prześlizgnie się niepostrzeżenie, ponieważ nie ma serii ataków po przeniknięciu, z którymi trzeba się uporać.

Na przykład, Moving Target Defense natychmiast zapobiega atakom, zanim będą miały szansę przeniknąć. Nie ma więc potrzeby ich wykrywania. A jeśli nie musisz wykrywać ataków, nie musisz monitorować, a jeśli nie musisz monitorować, nie musisz analizować. I tak dalej. Proste.

Łatwość użytkowania

Jest to całkiem proste do ocenienia: im więcej działań musi wykonywać produkt, żeby spełniał swoje zadanie, tym bardziej będzie Ci przeszkadzał i tym trudniej będzie go używać. Narzędzia, które monitorują i skanują lub zakotwiczają API, lub wdrażają politykę, mogą stanąć na drodze użytkownikom końcowym i wywołać konflikty z innymi narzędziami zapewniającymi bezpieczeństwo oraz z aplikacjami.

W modelu Moving Target Defense, rozwiązanie zmienia środowisko wykonawcze (run-time) i tworzy przynętę. I to wszystko. Praktycznie żadnego obciążenia, zakłóceń czy konfliktów. Oznacza to również, że DLL może być bardzo mała, tak żeby instalacja była trywialna i nie używano CPU podczas przetwarzania.

Ten rodzaj podejścia odciąża IT z niektórych jej największych bólów głowy związanych bezpieczeństwem i powstrzymuje użytkowników końcowych przed dzwonieniem do IT (helpdesk). Pomaga to również biznesowi. Otrzymuje wysoki poziom ochrony bez uciążliwych ograniczeń w zdroworozsądkowych działaniach biznesowych.

Szybkość i łatwość stosowania razem rozwiązują kwestie dotyczące negatywnych skutków operacyjnych prewencyjnej technologii bezpieczeństwa.

Moving Target Defense reprezentuje paradygmat “Ustaw i Zapomnij” i maksymę „Mniej znaczy więcej”. Zyskują zarówno IT jak i biznes.

Artykuł Artura Braunseteina z 19.10.2017r
po raz pierwszy opublikowany na Boardroom Events.