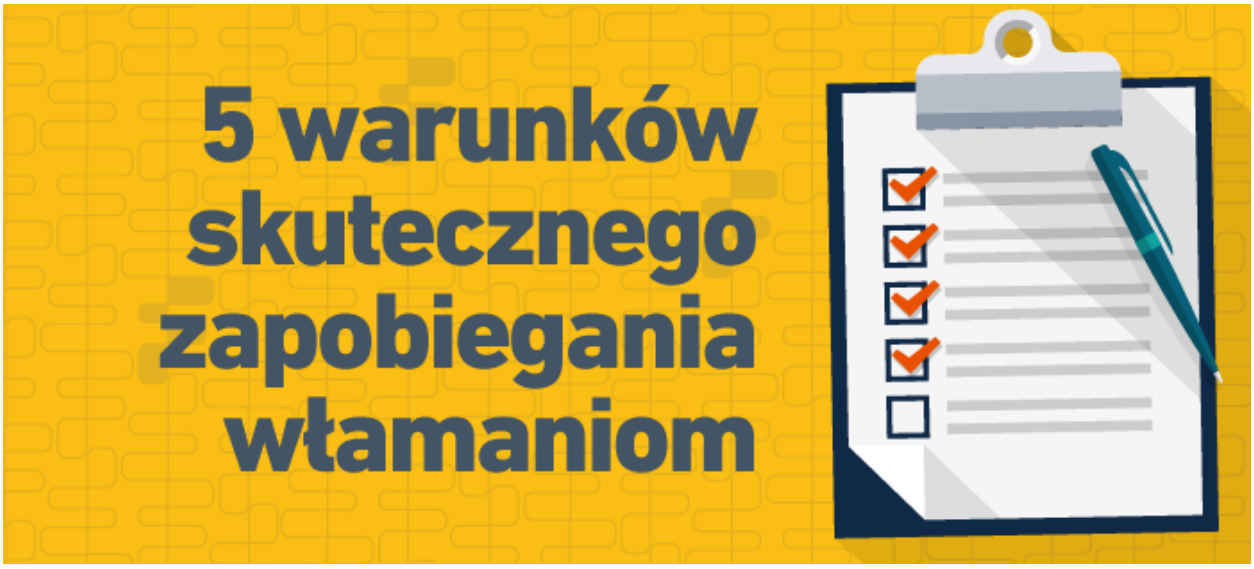
5 warunków skutecznego zapobiegania włamaniom.



Nie bez powodu nasze bagaże są prześwietlane na lotniskach. Jedynym sposobem na ustalenie, czy dany obiekt stanowi zagrożenie, jest zajrzenie do jego wnętrza.
Podobnie jest z zabezpieczeniami sieci. Jedynym sposobem na udaremnianie nowoczesnych ataków cybernetycznych jest dokładne sprawdzanie zawartości sieci w czasie rzeczywistym. I tak doszliśmy do pierwszego warunku, który musi być spełniony, aby się skutecznie bronić przed nowoczesnym atakiem.

Warunek 1. Dogłębny wgląd w zawartość sieci (nie tylko pakiety) w czasie rzeczywistym
Jak wykazaliśmy w pierwszym wpisie na blogu z tej serii („Czy dziś ponownie wybrał(a)byś ten sam system zapobiegania włamaniom?"), znaczna większość skutecznych ataków odbywa się nie na poziomie pakietów i ataków po stronie serwera, tylko na poziomie zawartości i ataków po stronie klienta — na przykład e-mail spear-phishingowy i stosowanie działających na dokumentach exploitów, które wykorzystują luki w zabezpieczeniach aplikacji komputerowych. Ataki tego typu nie są przepuszczane bezpośrednio. Wykorzystuje się w nich słabości natury ludzkiej. A te są absolutnie niewidoczne w pakietach.
W przypadku obrony przed atakami nowej generacji zawartość jest tym, czym były pakiety w tradycyjnych systemach zapobiegania włamaniom. Nowoczesny system zapobiegania włamaniom musi wykrywać w czasie rzeczywistym zagrożenia głęboko osadzone na poziomie zawartości i w razie czego podejmować działania obronne (blokady), tak jak to robią tradycyjne systemy zapobiegania włamaniom w odniesieniu do ataków na poziomie pakietów.
A jaki jest jedyny sposób na inspekcję zawartości w sieci? Trzeba odtwarzać, dekodować i analizować w locie całe sesje sieciowe (nie tylko pakiety). Tylko rozwiązania Fidelis to potrafią.
Prawdopodobnie zastanawiasz się, co mamy przeciwko pakietom. Ależ nic. Warto jednak wiedzieć, że zawartość i pakiety to dwie różne rzeczy — zwłaszcza z perspektywy obrony przed atakami. Tradycyjne systemy zapobiegania włamaniom potrafią analizować pakiety, ale nie sieciową zawartość.

W rozwiązaniach Fidelis stosujemy opatentowaną technologię o nazwie Deep Session Inspection®, która działa na poziomie sesji sieciowych, a nie pakietów, i zapewnia naszym produktom znacznie głębszy wgląd w zawartość przechodzącą przez sieć w czasie rzeczywistym niż ten oferowany przez tradycyjne systemy zapobiegania włamaniom. Umożliwia to nam wykrywanie zagrożeń na poziomie zawartości — niewidocznych dla tradycyjnych systemów zapobiegania włamaniom — i ich neutralizowanie.

Warunek 2. Widoczność, wykrywanie i zapobieganie na każdym etapie ataku

Nowoczesne ataki to całe procesy, a nie pojedyncze zdarzenia. Są to serie działań podejmowanych przez jakiś czas i realizowanych etapowo. Udaremnianie nowoczesnych ataków oznacza blokowanie atakujących zanim osiągną ostatecznych cel: kradzież, zniszczenie lub zaszyfrowanie danych ofiary.

Historia pokazuje, że nowoczesne ataki są trudne do wykrycia i jeszcze trudniejsze do odparcia. Koncentracja na jednej czy dwóch fazach ataku oznacza pewną przegraną. Aby udaremniać nowoczesne ataki, trzeba mieć możliwości wglądu, wykrywania i zapobiegania w każdej fazie ataku, również w fazie przygotowywania danych do celów przestępczych, a także ich wyprowadzania. Wymaga to wykrywania i blokowania atakujących we wszystkich fazach ataku — nie tylko podczas początkowego przenikania do środowiska, co jest jedynym etapem objętym kontrolą w przypadku tradycyjnych systemów zapobiegania włamaniom.

Warunek 3. Wykrywanie i zapobieganie w CZASIE RZECZYWISTYM oraz w PRZESZŁOŚCI

Jeśli ktokolwiek twierdzi, że jest w stanie wykryć — nie wspominając już o udaremnieniu— wszystkie ataki w czasie rzeczywistym, niewątpliwie mija się z prawdą.

Dlatego obrona przed atakami nowej generacji wymaga możliwości „cofania się w czasie", która pozwala stosować nowe informacje o zagrożeniach do przeszłych zdarzeń w sieci i punktach końcowych. Dzięki temu można wykrywać zagrożenia (i włamania), których szkodliwość nie była znana w czasie ich występowania.

Taka cybernetyczna podróż w czasie wymaga obszernej, nie wybiórczej pamięci zdarzeń w sieci. Oznacza to konieczność rejestrowania informacji (szczegółowych metadanych) o każdej sesji w sieci — bez względu na to, czy budzi ona podejrzenia, czy nie.

Tradycyjne systemy zapobiegania włamaniom skupiają się na wykrywaniu i zapobieganiu w czasie rzeczywistym. Nie mają nie wybiórczej pamięci ani funkcji umożliwiających analizy przeszłych zdarzeń. To prawdziwy problem, jeśli chodzi o obronę przed nowoczesnymi atakami.

W firmie Fidelis opracowaliśmy czekającą na opatentowanie technologię, która wydobywa, zapisuje i analizuje mnóstwo metadanych na poziomie protokołów, aplikacji i zawartości w każdej sesji przechodzącej przez sieć. Jak już wskazaliśmy w poprzednim wpisie na blogu, technologia ta umożliwia wykrywanie zagrożeń, które można dostrzec tylko wtedy, gdy szuka się wzorców zachowań w sieci występujących w dłuższej perspektywie i w ramach różnych sesji sieciowych. Stanowi to fundament procesu, który nazywamy „wykrywaniem zagrożeń opartym na danych", gdzie techniki uczenia maszynowego służą do wykrywania zagrożeń bez jakiejkolwiek uprzedniej wiedzy na ich temat.

Warunek 4. Rozszerzenie i weryfikacja zautomatyzowanych alertów

Tradycyjne systemy zapobiegania włamaniom często krytykuje się za „generowanie zbędnego szumu". Emitują one mnóstwo alertów, nie wskazując, które są najważniejsze. Nie udostępniają też wystarczająco dużo informacji, aby umożliwiać podejmowanie odpowiednich kroków. Jest to pewien problem w obliczu faktu, że większość zespołów ds. bezpieczeństwa zdecydowanie

cierpi na braki kadrowe.
System obrony przed atakami nowej generacji oszczędza czas dzięki automatycznej weryfikacji faktycznego występowania zagrożeń w punktach końcowych oraz udostępnianiu specjalistom ds. bezpieczeństwa wszelkich potrzebnych informacji o tym, co się działo przed alertem i po nim.
Warunek 5. Wszystkie powyższe w przypadku sieci ORAZ punktów końcowych
Ostatni wymóg. Bez względu na to, jak sprawnie wykrywasz zagrożenia w sieci, nigdy nie będziesz w stanie wykryć (ani udaremnić) wszystkich ataków wyłącznie dzięki analizie ruchu w sieci. Trzeba zwracać uwagę również na punkty końcowe. Atakujących, którzy obierają za cel dane, interesuje aktywność w punktach końcowych. Exploity są uruchamiane w punktach końcowych. Złośliwe oprogramowanie działa w punktach końcowych, gdzie pozostawia ślady i furtki. Naprawy są wykonywane w punktach końcowych.
To dlatego skuteczna obrona przed atakami nowej generacji wymaga funkcji uwidoczniania i blokowania ataków w punktach końcowych. Funkcje z poziomu punktów końcowych dostępne w rozwiązaniach Fidelis do zapobiegania włamaniom nowej generacji zapewniają tak samo głęboki wgląd, wykrywanie zagrożeń w czasie rzeczywistym, nie wybiórczą pamięć oraz możliwość wykrywania ataków w przeszłości, jakim dysponujemy w przypadku sieci. Ponadto dostępne są funkcje badań i napraw w punktach końcowych, które umożliwiają podejmowanie stosownych działań.
Wymienione pięć warunków nie są jedynymi, jakie musi spełniać skuteczne rozwiązanie obrony przed włamaniami, jednak są pięcioma najważniejszymi aspektami odróżniającymi systemy obrony przed atakami nowej generacji od tradycyjnych systemów zapobiegania włamaniom. System spełniający je wszystkie znacznie zwiększa szanse na udaremnianie ataków. Po dłuższą listę warunków, jakie muszą spełniać systemy obrony przed atakami nowej generacji, warto zajrzeć do najnowszego raportu z badań firmy Gartner, Defining Intrusion Detection and Prevention Systems.

— Kurt Bertone, dyrektor techniczny firmy Fidelis Cybersecurity