Wszystko, co musisz wiedzieć o ochronie punktów końcowych.

Przewodnik Net Complex.

Wprowadzenie do przewodnika.

Zabezpieczenie końcówki sieci nie jest już takie proste, jak kiedyś. Po pierwsze zabezpieczanie nie spoczywa już jedynie na *antywirusie*. Po drugie musimy sobie uświadomić, że zagrożenia, z którymi mamy na co dzień do czynienia, jak phishing czy ransomware, uległy diametralnym przemianom.

Motywy stworzenia poradnika:

> J*esteśmy w samym środku rewolucji w dziedzinie bezpieczeństwa punktów końcowych.*

A to dlatego, że dotychczasowe zabezpieczanie, jakie firmy od lat stosowały na swoich punktach końcowych instalując program antywirusowy, stało się powszechnie uważane za

niewystarczające. Pytanie, które się nasuwa, brzmi: **czego używać zamiast (lub oprócz) ochrony antywirusowej?**

Użytkownicy i ich punkty końcowe są postrzegane jako najbardziej narażone na cyberataki. Tymczasem zamiast aktywnie wzmacniać ochronę na zagrożonych punktach końcowych i unikać zainfekowania w pierwszej kolejności… wiele nowych rozwiązań ma za zadanie nakłonić przedsiębiorstwa by te zaakceptowały fakt, że zainfekowanie może się zdarzyć bez względu na to, co zrobią oraz że wyjściem z sytuacji jest inwestowanie w nowy schemat myślenia, a mianowicie skupienie na poprawie zdolności do wykrywania i reagowania na ataki - **po fakcie**.

> *Tymczasem oddanie pola walki cyberprzestępcom powinno stanowić OSTATECZNOŚĆ.*

Owszem, monitorowanie i narzędzia pierwszego reagowania, są cennymi elementami układanki, ale rozwiązania te koncentrują się i sprawdzają w dużych korporacjach, mających zespoły ekspertów zajmujących się tylko bezpieczeństwem i którzy mają czas i wiedzę w jaki sposób analizować wpisy zagrożeń i zakażeń. Zresztą…

> Czasem mimo zespołu ekspertów i tak jest za późno.

Bardzo dobrym przykładem jest ransomware. **Okazało się, że TeslaCrypt szyfruje i blokuje system plików w niecałą minutę.** To pozostawia właściwie zero czasu na reakcje. Dlatego zaleca się skoncentrowanie na zapobieganiu i zatrzymywaniu ataków jak najbliżej punktu początkowego.

Co dokładnie oznacza punkt końcowy – „endpoint"?

W języku cyberbezpieczeństwa endpoint czyli punkt końcowy może być dowolnym urządzeniem, które ma zdolność do łączenia się z siecią. Typowe przykłady to komputery stacjonarne, laptopy, smartfony, tablety, drukarki, terminale, itp.

Co oznacza termin „bezpieczeństwo punktów końcowych” - “endpoint security”?

Zawiera on w sobie wszelkie środki ochronne mające na celu zapobieganie i ograniczenie negatywnego wpływu na urządzenia końcowe. Większość ludzi gdy myśli o bezpieczeństwie punktu końcowego, myśli o antywirusie, jednak antywirus to nie wszystko.

Największe zagrożenia dla punktów końcowych:

- **Phishing:** ataki mające na celu nakłonienie użytkowników do kliknięcia złośliwych linków i załączników e-mail;
- **Spear phishing:** ukierunkowane ataki phishingowe, które wydają się wypływać ze źródeł, które znasz i którym ufasz;
- **Niełatanie luk:** błędy lub luki wykryte w oprogramowaniu, które mogą prowadzić do problemów związanych z bezpieczeństwem i exploitów;
- **Malvertising:** złośliwa kampania ataków, które dostarczają ładunki złośliwego oprogramowania, udając reklamy;
- **Drive-by-downloads:** ataki, które instalują złośliwe oprogramowanie na punkcie końcowym.

Przebieg ataku:

Ataki mogą przybierać różne kształty i formy. Aby uzyskać lepsze wyobrażenie o tym, jak mogą przebiegać, prześledźmy poniższy przykład:

VirLock RanSomware:

VirLock jest ransomwarem, który działa jako wirus pasożytniczy, infekuje pliki i rozprzestrzenia się do innych systemów, tworząc nowe, unikatowe wersje siebie.

Etap 1. Inicjacja:

Pracownik dostaje wiadomość e-mail, która, wydaje mu się, że pochodzi ze źródła, któremu ufa. Wiadomość zawiera link, w który pracownik klika. Link przekierowuje go na stronę internetową, która wydaje mu się nie znajoma. Nim pracownik się zorientuje, złośliwy kod wykorzystuje lukę w jego przeglądarce internetowej i pobiera kopię VirLock-a na jego komputer. W czasie gdy pracownik zamyka okno przeglądarki, VirLock jest już zainstalowany na jego komputerze.

Etap 2. Pełne odkrycie komputera końcowego:

A tymczasem na komputerze pracownika… VirLock przegrzebuje jego zasoby w poszukiwaniu konkretnych typów plików, takich jak pliki wykonywalne, pliki dokumentów, pliki

graficzne, pliki archiwów, itp. Po ich znalezieniu VirLock szyfruje pliki hosta, co czyni je już niedostępnymi dla pracownika. Ale to nie koniec. Infekuje również używając swojej ransomwarowości upload sieciowy, co prowadzi do dalszych infekcji. Oraz pozostawia jeszcze jeden plik wykonywalny. Potem blokuje ekran użytkownika, wyświetlając komunikat o naruszeniu praw autorskich i propozycji zapłaty okupu w celu odblokowania urządzenia i zaszyfrowanych plików. Wtedy jedynym sposobem jest zapłacenie grzywny w walucie bitcoin, albo zaakceptowanie faktu, że dane zostaną bezpowrotnie utracone.

Etap 3. Infekowanie dodatkowych punktów końcowych:

Ze względu na pasożytniczą naturę VirLock-a, obecność wielu zainfekowanych plików zwiększa szansę na rozprzestrzenienie się go w strukturze sieci firmowej danego pracownika. Z reguły pracownik nieświadomie sam wysyła zainfekowane pliki do swoich współpracowników. Co powoduje rozmnażanie się infekcji i blokowanie kolejnych maszyn w sieci.

Etap 4. Zakażenie całej sieci:

Ponieważ zakażenie VirLockiem następuje na całej maszynie, w końcu trafia na pracownika, który ma dostęp do zasobów dysku sieciowego. W ten sposób VirLock również tam się dostaje. A stamtąd już bardzo prosta droga do zainfekowania całej korporacji.

VirLock jest tylko jednym z przykładów złośliwego oprogramowania, które hakerzy wykorzystują na co dzień do obejścia zabezpieczeń i pogrzebania firm swoich ofiar. Firmy mogą wykorzystać szereg możliwości wykrywania prób ataku, reagować na atak czy też próbować odzyskiwać dane po infekcji, ale najlepszym sposobem na zminimalizowania szkód jest *zapobieganie infekcji,* o co należy zadbać w pierwszej kolejności.

Ochrona:

Ponieważ metody phishingu są jedną z najczęstszych metod dostarczania złośliwego oprogramowania, jedną z praktyk prewencyjnych jest **fachowe przeszkolenie użytkowników w zakresie wykrywania phishingu i wyuczenie ich nawyków zachowywania bezpieczeństwa**. Niestety pochłania to bardzo dużo czasu i generuje koszty a nie zawsze jest adekwatne do rezultatów. Poza tym nie zapominajmy, że nawet wyuczony pracownik może popełnić błąd. Dlatego tutaj powinna pojawić się ochrona punktów

końcowych - endpoint protection, która ma za zadanie wykryć próbę ataku na krótko przed tym, zanim malware wymknie się spod kontroli i zacznie zadawać konkretne obrażenia.

Korzyści z Endpoint Protection:

1. Zatrzyma ataki w momencie, w którym się zaczną: poprzez odcięcie infekcji zanim będzie miała szansę drastycznie się rozprzestrzeniać, co zmniejszy koszty i złożoność procedur związanych z odzyskiwaniem utraconych danych.

2. Wzmocni Twoje "najsłabsze ogniwo": jako ze punkty końcowe są najsłabszym ogniem naszej struktury bezpieczeństwa sieci firmowej, stosowanie zabezpieczeń na końcówce sieci znacznie wzmocni całość obronną.

3. Zapewni bezpieczeństwo użytkownikom sieci: każdy popełnia błędy, a jak już tak się stanie jednemu użytkownikowi, to endpoint protection ma za zadanie ochronić resztę firmy przed niepowołaną katastrofą.

4. Wstrzymywanie pracy maszyn: nawet mając tylko jedno urządzenie wyłączone z eksploatacji, może to być kosztowne dla firmy. Silna ochrona punktów końcowych pozwala uniknąć przestojów i utrzymać dostęp ważnych układów i plików w strukturze firmy.

Punkty końcowe są pierwszą linią obrony. Zatrzymają ataki i zmniejszą ryzyko naruszenia danych lub infekcji całej firmy. Szkolenie w zakresie bezpieczeństwa w połączeniu z wysokim poziomem ochrony punktów końcowych jest niezbędne do ochrony zarówno części jak i całości organizacji.

Ewolucja Endpoint Security

Ochrona końcówek przeszła naprawdę długą drogę od zwykłego antywirusa.

Jeśli od razu pomyślałeś o antywirusie po usłyszeniu terminu „ochrona punktu końcowego”, nie martw się, nie jesteś jedyny. Mają ze sobą bliski związek, ale tylko przy założeniu, że na bezpieczeństwo ochrony punktu końcowego składa się skanowanie systemu i instalowanie na nim aktualizacji.

Zanim spojrzymy na najnowsze osiągnięcia w zakresie ochrony punktu końcowego, przyjrzyjmy się dlaczego i jak ta technologia ewoluowała.

Powstanie i upadek technologii Endpoint Protection opartej na sygnaturach:

Do niedawna ochroną punktu końcowego było zainstalowanie oprogramowania, które miało za zadanie skanować pliki i porównywać je w swojej bazie danych na zasadzie: czy dany plik jest złośliwy czy nie - podobnie do identyfikacji przestępców po odcisku palca. Co na to atakujący? Przez jakiś czas pozwalało to firmom być o jeden krok przed atakującymi. Dlatego też cyberprzestępcy zaczęli tworzyć nowe złośliwe oprogramowanie mające za zadanie infekować jak największą ilość maszyn - nim zostaną wykryte. Wtedy firmy zajmujące się rozwiązaniami do ochrony sieci zaczęły walczyć o próbki takiego oprogramowania, by stworzyć ich odcisk (sygnaturę) i dodać go do swojej bazy. Z kolei atakujący zaczęli tworzyć kolejne wersje, których nie było w bazie. I tak w koło Macieju.

Podsumowując przestępcy zaczęli opracowywać nowe mechanizmy szyfrowania i wprowadzali niewielkie, ale liczne zmiany w kodzie złośliwego oprogramowania. To pozwoliło na tworzenie niezliczonych klonów i odmian programów, z których każdy miał unikalny odcisk palca.

Pozostawiając użytkowników narażonymi na nowe wariacje szkodliwego oprogramowania, firmy specjalizujące się w ochronie miały duży kłopot… Nie wyrabiały z aktualizowaniem sygnatur oprogramowania antywirusowego na końcówce sieci. Potrzeba matką wynalazków.

Jak ochronić punkty końcowe mojej firmy przed nowymi i zaawansowanymi atakami?

- **Wykrywanie złośliwego oprogramowania przed zainfekowaniem.**

Identyfikowanie nowej próbki, tworzenie jej sygnatury i dodawanie jej do listy zablokowanych wymaga czasu. W tym okresie firmy są narażone na zagrożenie.

Jednym ze sposobów minimalizacji ataku jest gromadzenie wiedzy o zagrożeniach z wielu źródeł i szukanie nowych zdarzeń związanych z atakami i bezpieczeństwem. Robi się to niemal w czasie rzeczywistym, co umożliwia monitorowanie stanu bezpieczeństwa. Problem jednak nie znika, tak samo jak w przypadku ochrony opartej na sygnaturach. Niestety: aby wykryć atak, musi dojść do udanego ataku na co najmniej jednej ofierze. Cóż, Szekspir sam ciśnie się na usta: **„Niech ryczy z bólu ranny łoś,/ Zwierz zdrów przebiega knieje,/ Ktoś nie śpi, aby spać mógł ktoś./ To są zwyczajne dzieje”.**

- **Analiza behawioralna. Wykrywa złośliwe oprogramowanie podczas próby wykonania.**

Podczas gdy podpis danego malware może się często zmieniać, esencja złośliwego oprogramowania zazwyczaj działa tak samo. Zatem poprzez monitoring szkodliwych programów w czasie rzeczywistym, wykorzystując tak zwaną metodę behawioralną, jesteśmy w stanie wykryć objawy prób działania szkodliwego oprogramowania i natychmiast je zablokować, nim spróbują wykonać jakieś szkody. Zamiast gonić za próbkami złośliwego softu, by dodać je do czarnej listy (cóż, 390.000 próbek generowanych dziennie), prościej stworzyć blokowanie jednego zachowania, co da możliwość zablokowania wielu szkodliwych programów. Teraz oraz w przyszłości.

- **Biała i czarna lista.**

Jako kontrolę administracyjną zaleca się stworzenie list programów i aplikacji, z których może korzystać użytkownik końcowy. Ogranicza to możliwość odpalenia programów niepowołanych. System czarnej i białej listy sprawdza się dobrze w małych firmach. Natomiast budowanie jej struktury w dużych korporacjach jest dość skomplikowane i czasochłonne.

- **Sandboxing.**

Najlepszym sposobem by w ostateczny sposób określić czy dany program jest malwarem, to po odpalić go i zobaczyć co zrobi. Najlepiej robić to z dala od rzeczy, których nie chcesz stracić.

Do tego właśnie służą programy typu piaskownica – sandbox – czasem nazywane kontenerami. Tworzą one izolowane środowisko, w którym można bez uszkadzania systemu nadrzędnego odpalać, tj. testować, nieznane pliki. Podczas testowania pliku jesteśmy w stanie powiedzieć, jak dany plik będzie się zachowywać. Problem piaskownicy polega na tym, że malware może powiedzieć, że nie ujawnić się w środowisku wirtualnym. Wiedząc że jest w piaskownicy może ukryć swoje złośliwe atrybuty. Rozwiązanie sandboxingu nie ma wygórowanych wymagań w zakresie zasobów systemowych. Natomiast wymaga analizy oraz pracowników chętnych do uruchomienia go i monitorowania jego zachowania.

- **Endpont Protection - pakiet**

Ogólnie panującą mądrością jest twierdzenie, że dobre zabezpieczanie to warstwowe zabezpieczenie. Nie można powiedzieć, że jedno rozwiązanie jest idealne i wszechogarniające. Aby skutecznie chronić firmę przed szerokim spektrum ataków, należy zainwestować w wiele różnych metod, stosując połączoną ochronę przed zagrożeniami. Metody te muszą zawierać się w – zapobieganiu, wykrywaniu i reagowaniu.

Chroń swoją sieć przez:

Zapobieganie:

- tworzenie polityk i ograniczanie dostępu do naszych punktów końcowych (**firewall**);

- regulacja aplikacji uruchamianych na punktach końcowych (**czarna i biała lista**);

- identyfikowanie i blokowanie malware'u, który próbuje wykonać atak na punkt końcowy **(endpoint protection)**;

- dokonywanie aktualizacji systemu końcowego, by uchronić przed powstaniem luk;

- szkolenia użytkowników końcowych, by obudzić w nich świadomość zagrożenia i nauczyć ich nawyków bezpieczeństwa.

Wykrycie:

Sposoby pozwalające nam określić czy bezpieczeństwa zostało naruszone czy nie:

- identyfikowanie anormalnego zachowania (zagrożenie / wykrywania anomalii);

- monitorowanie logów (SIEM);

- zidentyfikowanie nieautoryzowanego lub podejrzanego dostępu.

Reagowanie:

Jakie kroki należy podjąć, by być pewnym, że jesteśmy przygotowani na atak:

- wyraźnie określić, co stanowi naruszenie polityki bezpieczeństwa oraz kto w przypadku jej naruszenia ma być powiadomiony;

- utworzenie wygodnych funkcji tworzenia kopii zapasowych i odzyskiwania danych z tych kopii;

- opracowanie procedur czy i w jakim wypadku pojawiającego się cyberzagrożenia/ ataku powiadomić klientów, pracowników, doradców prawnych czy organy ścigania cyberprzestępców.

Bibliografia:
Magic Quadrant for Endpoint Protection Platforms
www.barkly.com
Blog Net Complex