Rozwiązanie Cisco Ransomware Defense: trzymaj oprogramowanie ransomware na dystans

A gdyby Twoja firma mogła lepiej zabezpieczyć się przed oprogramowaniem ransomware niezależnie od sposobu ataku? Tylko Cisco oferuje odpowiednie zabezpieczenia i właściwą architekturę.

Omówienie

Pliki i informacje są siłą napędową organizacji. Konieczność zapewnienia, by dane te – oraz wydajność organizacji – pozostawały nietknięte i bezpieczne to kwestia niepodlegająca dyskusji.

Coraz częściej pojawia się jednak ransomware, złośliwe oprogramowanie, które blokuje informacje (np. dokumenty, zdjęcia i muzykę) na komputerze osoby lub organizacji. Blokada jest zdejmowana dopiero wówczas, gdy użytkownik zapłaci okup za odzyskanie plików. Bez odpowiednich zabezpieczeń ransomware może spowodować ogromne szkody, zmuszając organizację do funkcjonowania jak w czasach przed pojawieniem się komputerów.

Ransomware często przedostaje się poprzez pakiety wykorzystujące luki w zabezpieczeniach (tzw. exploit kits), złośliwe reklamy (zarażone reklamy na stronach internetowych, w których może kryć się złośliwe oprogramowanie), ataki typu phishing (fałszywe wiadomości e-mail udające wiadomości godne zaufania) lub kampanie spamowe. Atak może zacząć się od kliknięcia łącza lub załącznika w fałszywej wiadomości e-mail. Zdarza się także, że użytkownik otwiera stronę ze złośliwą reklamą, która automatycznie zaraża komputery.

Poznaj rozwiązanie Cisco® Ransomware Defense. Zmniejsza ono ryzyko związane z zarażeniem przez oprogramowanie ransomware poprzez zastosowanie metody warstwowej – działa od warstwy DNS przez punkt końcowy po sieć organizacji, pocztę e-mail i sieć WWW. Oferujemy zintegrowane zabezpieczenia oparte na architekturze łączącej niezrównany wgląd w informacje z doskonałym reagowaniem na oprogramowanie ransomware.

Korzyści

- **Niższe ryzyko związane z oprogramowaniem ransomware**, dzięki czemu możesz skupić się na działalności biznesowej
- **Natychmiastowa ochrona** dzięki zabezpieczeniom blokującym zagrożenia, zanim będą mogły podjąć próbę opanowania komputerów
- **Niezrównana widoczność i sprawne reagowanie** dzięki metodzie opartej na architekturze, obejmującej zarówno warstwę DNS, jak i sieć oraz punkt końcowy
- **Zapobieganie poziomemu rozprzestrzenianiu się złośliwego oprogramowania** dzięki silnej segmentacji sieci
- **Możliwość korzystania z zasobów badawczych** i analitycznych odnośnie ransomware czołowej w branży grupy Talos.

Dynamicznie rozwijające się, potężne zagrożenie

Ten rok należy do oprogramowania ransomware. Przynosi ono naprawdę wysokie zyski. Ransomware szybko stało się jednym z najbardziej lukratywnych typów złośliwego oprogramowania.

FBI twierdzi, że wkrótce wartość tego rynku sięgnie miliard dolarów rocznie. Jak wynika z badania Cisco Talos, jedna kampania ransomware może przynieść nawet 60 mln USD zysku rocznie. O ransomware robi się coraz głośniej – temat ten pojawia się nawet w programach telewizyjnych.

Przestępcy dysponują odpowiednimi środkami i starają się opracowywać nowe, jeszcze skuteczniejsze techniki. Naszym zdaniem ransomware w przyszłości będzie lepiej się samopowielać, aby blokować rozległe obszary sieci firmowych. W efekcie pod względem funkcjonalności IT organizacja wróciłaby do lat 70. XX w.

Aktualne zabezpieczenia przed oprogramowaniem ransomware to głównie produkty jednopunktowe. Biorąc pod uwagę różnorodność dróg zarażenia, musimy zastanowić się nad podejściem w większym stopniu uwzględniającym całość architektury.

W niniejszym omówieniu rozwiązania wzięto pod uwagę różne wektory i metody stosowane przez przestępców. Obrońcy muszą zabezpieczyć zarówno pocztę e-mail, jak i sieć WWW, zablokować dostęp do złośliwej infrastruktury w Internecie, zatrzymać pliki oprogramowania ransomware usiłujące przedostać się do punktu końcowego, zablokować próby przekazania sterowania i nadzoru, a w przypadku, gdy dojdzie do zarażenia, zapobiec łatwemu poziomemu przepływowi złośliwego oprogramowania.

Co kupujesz

Rozwiązanie Cisco Ransomware Defense obejmuje wszystkie niezbędne elementy architektury zabezpieczeń Cisco umożliwiające rozwiązanie problemów związanych z oprogramowaniem ransomware. Można wybrać wszystkie składniki lub tylko niektóre, zgodne z najbardziej pilnymi potrzebami w zakresie bezpieczeństwa.

Pakiet Ransomware Defense obejmuje:

- Cisco Umbrella, rozwiązanie blokujące zagrożenia w warstwie DNS, daleko od sieci
- Cisco Advanced Malware Protection (AMP) for Endpoints, rozwiązanie blokujące złośliwe pliki ransomware, uniemożliwiające uruchamianie ich w punktach końcowych.
- Cisco Email Security (w chmurze i po stronie klienta), rozwiązanie zatrzymujące fałszywe wiadomości (phishing) i spam stanowiące próbę dostarczenia oprogramowania ransomware

- Advanced Malware Protection, rozwiązanie, które można natychmiast dodać do zabezpieczeń poczty e-mail przy użyciu łatwej licencji na potrzeby statycznych i dynamicznych (sandboxing) analiz nieznanych załączników przenikających przez bramę Cisco zabezpieczającą pocztę e-mail
- Cisco Firepower™, zaporę nowej generacji (NGFW) blokującą ruch związany z przekazaniem sterowania i nadzoru oraz wszystkie złośliwe pliki przenikające do sieci
- Cisco ISE, rozwiązanie, które poprzez sieć Cisco dynamicznie dzieli sieć na segmenty, dzięki czemu oprogramowanie ransomware nie może rozprzestrzeniać się poziomo

Przy użyciu rozwiązania Ransomware Defense organizacje mogą wykorzystywać sieć jako element egzekwowania zasad, ograniczający rozprzestrzenianie się oprogramowania ransomware. Nawet jeśli dojdzie do infekcji, utrudni to powielanie złośliwych programów w sieci.

Usługi Cisco Security Services mogą przeprowadzić błyskawiczną ocenę sytuacji w ramach reagowania na zdarzenia po wybuchu epidemii. Upraszczają one także wdrożenie rozwiązań, m.in. AMP i NGFW.

Najważniejsze funkcje

- Blokowanie oprogramowania ransomware uniemożliwiające przedostanie się do sieci lub pobranie na laptopy
- Ograniczanie zasięgu oprogramowania ransomware w razie, gdyby doszło do ataku

Usługi zabezpieczeń ułatwiają walkę z oprogramowaniem ransomware

Zespół ds. reagowania na zdarzenia Cisco Security Services może zaoferować zarówno usługi gotowości reagowania na zdarzenia oraz reaktywnego reagowania na zdarzenia w przypadku wybuchu epidemii oprogramowania ransomware.

Ponadto usługi Cisco Security Integration Services pomagają rozwiązywać problemy z architekturą na poziomie rozwiązania. Upraszczają one wdrożenie technologii rozwiązań, takich jak AMP dla punktów końcowych i Cisco Firepower NGFW. Nasz zespół dysponuje głęboką wiedzą na temat udostępniania rozwiązań zintegrowanych zabezpieczeń, aby przyspieszyć wdrożenie potrzebnej technologii przy jak najmniejszych zakłóceniach.

Patrząc szerzej, organizacje muszą także dysponować właściwą technologią i zasadami archiwizowania danych, aby zabezpieczyć się przed skutkami zarażenia oprogramowaniem ransomware.

„Zabezpieczyliśmy się przed ogromnym niebezpieczeństwem związanym z atakami oprogramowania ransomware przez sieć WWW oraz zdecydowanie ulepszyliśmy środowisko użytkownika w zakresie łączności z Internetem.”

– Octapharma

Cisco Capital

Finansowanie pozwalające na realizację celów

Rozwiązania finansowe Cisco Capital® mogą pomóc w pozyskaniu technologii niezbędnych do realizacji celów i uzyskaniu przewagi nad konkurencją. Możemy pomóc w obniżeniu wydatków kapitałowych. Przyspiesz swój rozwój. Zoptymalizuj wydatki inwestycyjne i stopę zwrotu z inwestycji. Finansowanie Cisco Capital zapewnia elastyczność w nabywaniu urządzeń, oprogramowania, usług i dodatkowego sprzętu innych firm. Wnosisz tylko jedną, przewidywalną opłatę. Usługi Cisco Capital są dostępne w ponad 100 krajach. Dowiedz się więcej.

Przewaga Cisco

Oprogramowanie ransomware będzie próbować przeniknąć do Twojej organizacji w każdy możliwy sposób. Oszukańcze wiadomości e-mail, zarażone banery internetowe, spam – trzeba zabezpieczyć wiele ścieżek. Tylko Cisco oferuje architekturę zabezpieczeń pozwalającą na skuteczną walkę z ransomware. Produkty chroniące pojedyncze punkty nie wystarczą. Za naszym rozwiązaniem stoi czołowa w branży grupa badawcza Talos, która przeprowadziła wszechstronne badania na temat zagrożeń jakie niesie ransomware. To najlepsza gwarancja skuteczności naszej warstwowej ochrony. Zablokujemy oprogramowanie ransomware, a jeśli uda mu się wniknąć do sieci poprzez luki w zabezpieczeniach, co niestety może się zdarzyć – pokonamy je.

C22-737492-01 08/16