CASE STUDY

Kancelaria DZP wykorzystuje rozwiązanie Cynet360 do uszczelnienia stosowanych systemów zabezpieczeń przed ransomware i atakami APT.

KLIENT

Kancelaria Prawna Domański Zakrzewski Palinka jest jedną z największych, niezależnych polskich kancelarii prawnych, zatrudniającą ponad 250 osób. Posiada biura w Warszawie, Poznaniu, Wrocławiu i Londynie. Jej czołową pozycję potwierdzają rankingi najlepszych kancelarii prawnych publikowane przez Rzeczpospolitą, Dziennik Gazetę Prawną oraz specjalistyczne rankingi międzynarodowe: Chambers & Partners, Legal 500, IFLR1000, ITR WorldTax i WTR1000.

OCZEKIWANIA KLIENTA

Ataki cyberprzestępców są kierowane na firmy i instytucje wielu branż. Kancelarie prawne ze względu na specyfikę prowadzonej działalności i poufność oraz potencjalną wartość przechowywanych i przesyłanych informacji są szczególnie „atrakcyjnym" celem. Ujawnienie tych informacji może mieć bardzo negatywne skutki - zarówno dla kancelarii, jak i jej klientów. Atakujący korzystają z różnorodnych scenariuszy ataku – przykładem ataku socjotechnicznego jest sytuacja, w której kilkanaście kancelarii prawnych otrzymało informację o planowanej kontroli Generalnego Inspektora Ochrony Danych Osobowych. Niebezpieczna wiadomość nie została wysłana z serwera GIODO i zawierała złośliwe oprogramowanie szyfrujące dane na komputerze. Odszyfrowanie danych wiązało się z koniecznością zapłaty kwoty 200 dolarów.

Liczący 10 osób dział IT Kancelarii jest świadomy aktualnych zagrożeń i stale aktualizuje wiedzę zarówno z zakresu najnowszych ataków, jak i dostępnych na rynku rozwiązań zapewniających skuteczną ochronę.

Firma stosuje kilka rozwiązań podnoszących bezpieczeństwo organizacji. Komunikacja pracowników, którzy przebywają poza firmą odbywa się z wykorzystaniem tunelu VPN oraz certyfikatów do szyfrowania korespondencji. Na komputerach zainstalowano oprogramowanie antywirusowe jednego z wiodących na rynku producentów, dodatkowo firma korzysta z zaawansowanego rozwiązania, które analizuje cały ruch sieciowy pod kątem malware i innych form ataków APT.

W celu maksymalnej ochrony danych powierzonych przez Klientów Kancelarii, Dyrektor Działu IT – Marek Laskowski zdecydował o potrzebie wdrożenia dodatkowego systemu, który zabezpieczy pracowników przed najnowszymi zagrożeniami, w tym rozszerzającymi się na coraz większą skalę atakami typu ransomware.

Większość używanych do tej pory przez DZP rozwiązań do ochrony infrastruktury pochodziła od jednego, popularnego i docenionego przez firmę Gartner producenta. Sprawują się one bardzo dobrze, jednak zgodnie z najlepszymi praktykami w zakresie bezpieczeństwa IT i zaleceniami firm analitycznych postanowiono zdywersyfikować stosowane narzędzia do ochrony.

Cynet umożliwia detekcję zakamuflowanych, zmutowanych i nieznanych form malware, które przedostały się przez inne formy zabezpieczeń.

ROZWIĄZANIE

Za realizację projektu odpowiedzialne były 2 osoby – Roman Osiński, Network & Security IT Administrator oraz jego przełożony, wspomniany wcześniej Dyrektor IT Marek Laskowski. Spośród kilku branych pod uwagę narzędzi wybrano rozwiązanie Cynet-360, system typu ETDR (Endpoint Detection and Response), który realizuje 2 podstawowe zadania:

- identyfikuje zagrożenia w oparciu o tzw. identyfikatory kompromitacji (IoC)
- usuwa lub blokuje złośliwe oprogramowanie z wykorzystaniem agentów działających na stacjach końcowych.

Decydując się na rozwiązanie Cynet zwrócono uwagę na dwa wyróżniające go elementy. Pierwszym są tzw. „deception technologies" - techniki wzbudzające do działania wyrafinowany malware poprzez „podrzucanie" mu plików-pułapek (tzw. honeypots) udających wrażliwe dane i pliki. Cynet generuje, a następnie monitoruje tego typu zasoby i w momencie stwierdzenia próby uzyskania do nich dostępu, przeszukuje całe środowisko IT wykrywając identyczne identyfikatory, a następnie usuwa malware ze wszystkich zainfekowanych stacji.

Analogiczne działanie podejmowane jest w przypadku ransomware - gdy któryś z plików pułapek zostanie zaszyfrowany, Cynet natychmiast przystępuje do unieszkodliwienia zagrożenia.

Drugim szczególnym istotnie wyróżniającym Cynet na tle konkurencji elementem, który zwrócił uwagę zespołu jest oferowana wraz z rozwiązaniem usługa Security Operation Center (SOC). Obejmuje ona całodobową pomoc ekspertów firmy Cynet, która może być nieoceniona w przypadku wystąpienia sytuacji kryzysowej. Specjaliści reprezentujący producenta przeanalizują zagrożenia, doradzą najskuteczniejsze formy ich wyeliminowania oraz pomogą uszczelnić systemy bezpieczeństwa na przyszłość.

WDROŻENIE

Po przeprowadzonych testach zdecydowano się na wdrożenie rozwiązania na wszystkich stacjach wykorzystywanych w organizacji. Pierwszym krokiem było wdrożenie modułu zarządzającego wraz z bazą danych do zbierania informacji w wykorzystaniem serwera MS Windows. Z poziomu centralnego serwera zainstalowano zdalnie agentów, odpowiadających za monitorowanie 229 urządzeń końcowych i przekazywanie informacji do centralnej bazy danych. Agenci działają w postaci procesu systemu operacyjnego i są niezauważalni dla użytkownika. Aby zapewnić użytkownikom wydajną pracę wykorzystano

funkcję umożliwiającą zdefiniowanie stopnia maksymalnego obciążenia procesora danego urządzenia. Dzięki unikalnym mechanizmom współpracy klient – serwer, wdrożenie zajęło kilka godzin. Wykorzystywane przez Cynet mechanizmy pozwoliły też uniknąć problemów ze sterownikami, niekompatybilnością z innymi agentami czy aplikacjami oraz ryzyka wystąpienia tzw. blue screens.

ZASADA DZIAŁANIA

Wykrywanie zagrożeń rozpoczyna się skanowaniem zasobów korporacyjnych, w tym punktów końcowych, użytkowników, plików i sieci. Wyniki są gromadzone w bazie danych.

Kolejnym etapem jest analiza zebranych danych – są one filtrowane i analizowane za pomocą różnych metod statystycznych. Cynet identyfikuje anomalie lub zmiany w konfiguracji sieci, modyfikacje lub zmiany systemu plików, rejestru, podejrzane aktywności użytkowników lub ich komputerów. Wykorzystuje automatyczną analizę wielostopniową, aby potwierdzić poziom zagrożenia i ryzyka. W sytuacji, gdy zagrożenie nie zostało ustalone z całą pewnością, jest automatycznie przekierowywane do SOC, gdzie zespół ekspertów dokonuje ostatecznej oceny zagrożenia co pozwala ograniczyć do minimum ilość tzw. false-positives.

W przypadku, gdy SOC potwierdzi wystąpienie zagrożenia, administrator systemu jest automatycznie powiadamiany za pośrednictwem panelu zarządzania rozwiązania Cynet, może też otrzymać alert w formie wiadomości e-mail, a w niektórych przypadkach inżynierowie SOC Cynet kontaktują się bezpośrednio z inżynierami bezpieczeństwa klienta. Stosowny komunikat może zostać także wysłany do systemu SIEM.

Cynet umożliwia stosowanie różnych metody niwelowania zagrożenia - kwarantannę lub usunięcie plików, odłączenie użytkownika od sieci, wyłączenie systemu, uruchomienie określonej komendy. Każdy podejrzany plik można niezależnie wysłać do SOC lub sandboxa w celu szczegółowej jego analizy. Ciekawą funkcją jest auto-remediacja – w przypadku pojawienia się podobnego alertu administrator systemu może zdefiniować, aby od tego momentu system sam podejmował określoną akcję.

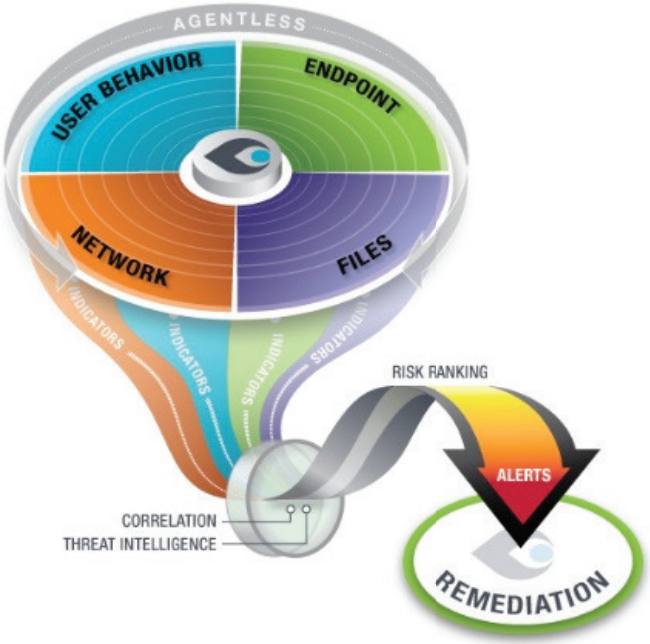
PO WDROŻENIU – PODSUMOWANIE

Rozwiązanie Cynet360 dzięki unikalnemu podejściu do wykrywania zagrożeń stanowi kolejny element zabezpieczenia Kancelarii przed zakamuflowanymi, zmutowanymi i nieznanymi formami malware na wypadek, gdyby przedostały się przez inne systemy zabezpieczeń stosowanych przez DZP.

Wdrożenie systemu zajęło kilka godzin, a dostępność podczas wdrożenia inżynierów producenta oraz partnera – firmy Passus pozwoliły dopasować rozwiązanie do indywidualnych potrzeb Klienta. Dla kilkuosobowego działu IT firmy DZP bardzo cenna okazała się usługa 24-godzinnego wsparcia ekspertów Security Operation Center, dzięki czemu nie dopuszczono do sytuacji kryzysowych, ale i ograniczono ilości zgłoszeń false-positives. Przypadki fałszywych alarmów niepotrzebnie zajmują czas i zasoby organizacji, a sposób działania Cynet360 w połączeniu z usługą SOC pozwala na znaczne ich ograniczenie.

W przypadku wykrycia zagrożeń, krytyczne staje się ich jak najszybsza identyfikacja i skuteczne wyeliminowanie.

Właściwe wdrożenie i konfiguracja Cynet pozwala usunąć zagrożenia za pomocą „jednego kliknięcia" i/lub stworzonej automatycznej reguły. Reakcja zajmuje wtedy sekundy, a nie godziny lub dni, skracając ryzyko propagacji infekcji w obrębie organizacji.



Cynet wykorzystuje unikalne metody detekcji zagrożeń, korelacji i analizowania wskaźników w obszarze plików, użytkowników, sieci oraz urządzeń końcowych.

PASSUS SA

Passus Spółka Akcyjna jest polskim producentem, integratorem i dostawcą wysoko specjalizowanych rozwiązań informatycznych obejmujących w szczególności:

- rozwiązania do monitorowania i rozwiązywania problemów z wydajnością sieci oraz aplikacji;
- rozwiązania z zakresu bezpieczeństwa IT m.in. do wykrywania podatności, zabezpieczenia sieci, aplikacji oraz danych przed zaawansowanymi atakami oraz zagrożeniami wskutek nadużyć lub zaniedbań wewnętrznych;
- rozwiązania do projektowania, budowy i modernizacji wydajnych sieci WiFi w tym realizacji specjalistycznych projektów „pod klucz" (m.in. captive portal, lokalizacja zasobów, dostęp WiFi w środkach komunikacji i transportu);
- narzędzia interpretujące dane w ruchu sieciowym, logach oraz bazach danych, które pozwalają wyodrębnić określone pliki, treści lub metadane, które mogą być następnie przesłane do zewnętrznych systemów analitycznych, takich jak SIEM czy antyfraud;
- rozwiązania do optymalizacji i konsolidacji infrastruktury serwerowej;
- rozwiązania zabezpieczające przed nadużyciami finansowymi (antyfraud).

Tym, co wyróżnia Passus SA spośród firm integracyjnych, jest elastyczność i koncentracja na rzeczywistych potrzebach Klienta. Płaska i przejrzysta struktura organizacyjna spółki oraz ograniczone do niezbędnego minimum procedury pozwalają szybko i skutecznie reagować na oczekiwania Klienta. Ponad 20 lat współpracy z firmami oraz instytucjami z Polski i z zagranicy zaowocowało znajomością uwarunkowań biznesowych i technicznych tych organizacji. Do grona Klientów w Polsce należą tak wymagający partnerzy, jak m.in. Ministerstwo Obrony Narodowej, T-Mobile, Narodowy Bank Polski, Grupa Enea, Centrum Onkologii w Gliwicach, Komisja Nadzoru Finansowego, Orange, PGE, Swedwood, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

Bazując na własnych produktach i usługach oraz technologiach uznanych światowych producentów, Passus SA tworzy i wdraża rozwiązania, precyzyjnie dostosowane do wymagań klienta. Spółka zapewnia klientom kompleksową obsługę, począwszy od analizy potrzeb, przez planowanie, usługi wdrożeniowe, szkolenia pracowników, aż po opiekę serwisową oraz posprzedażną. Oferowane rozwiązania są przygotowywane w oparciu o produkty własne jak i uznanych światowych dostawców. Firma jest partnerem takich producentów jak: Riverbed (Riverbed Premier Partner), Core Security (wyłączny dystrybutor w Polsce), Fidelis Cybersecurity (rekomendowany Partner w Polsce), NetScout, Cisco (Premier Partner), FlowMon (Gold Partner), Symantec oraz Qualys. Passus posiada także własny zespołów programistów i inżynierów realizujących projekty na indywidualne zamówienie. Na bazie zebranych doświadczeń, w maju 2014 roku, zespół ten przygotował unikalne w skali światowej rozwiązanie umożliwiające identyfikację nadużyć i incydentów w oparciu o analizę ruchu sieciowego - Passus Ambience.

Firma Passus SA powstała w wyniku wydzielenia Działu Sieci i Bezpieczeństwa IT z Passus sp. z o.o., działającej w branży IT od 1992 roku. Zatrudnia blisko 30 wykwalifikowanych pracowników – inżynierów, programistów i specjalistów. Potwierdzeniem kompetencji zespołu, obok wielu udanych wdrożeń, jest blisko 40 indywidualnych certyfikatów m.in.: poświadczenie bezpieczeństwa osobowego do klauzuli „Tajne" oraz „NATO Secret", CISA, CISSP, Riverbed Certified Solutions Professional, Cisco Associate oraz Professional w zakresie R&S (routing & switching), Security oraz Wireless, Core Impact Certified Professional, Audytor wiodący ISO 27001, Riverbed Network and Application Performance Management Qualified Trainer oraz Fluke Networks Application Performance Appliance Certified Trainer. W 2017 roku firma spełniła wymagania stawiane przez Agencję Bezpieczeństwa Wewnętrznego i uzyskała **świadectwa bezpieczeństwa przemysłowego**, które potwierdzają zdolność spółki do realizacji usług w instytucjach i gałęziach przemysłowych związanych z dostępem do informacji niejawnych - krajowych jak i NATO oraz Unii Europejskiej.