KRAJOBRAZ CYBERZAGROŻEŃ W SEGMENCIE HANDLU DETALICZNEGO
NISKA ŚWIADOMOŚĆ = WYSOKIE RYZYKO

Każdy duży incydent, generuje nagłówki w czasopismach branżowych oraz „dużych gazetach" o zasięgu ogólnokrajowym, które pociągają za sobą pytanie o bezpieczeństwo, zarówno kont pojedynczego użytkownika, jak i całych systemów płatniczych.

Kart kredytowych, stanowiących w dzisiejszym świecie swego rodzaju walutę, dotyczy podobny problem, co banknotów - niewystarczająca siła zabezpieczeń.

W zasadzie tylko niekorzystny bilans ekonomiczny (zbyt duży nakład pracy w stosunku do zakładanych zysków), oraz konsekwencje prawne związane z wykryciem, powstrzymują hakerów od popełniania przestępstw. Niestety jest coraz więcej takich obszarów, które zostają skutecznie inwigilowane i profesjonalnie rozpracowane.

Jednym z takich obszarów, jest struktura transferu informacji, pomiędzy klientem a dostawcą usługi/towaru. Cyberprzestępcy uważają, że korzystniej jest włamać się do serwera, w którym przechowywane są dane kart płatniczych, niż do banku po gotówkę.

Dlaczego to jest ważne dla sieci handlowych? Dlatego, że priorytetem, jest ochrona relacji z klientami, którzy codziennie zaopatrują się u nich w najrozmaitsze dobra.

Budowanie i utrzymanie zaufania na rynku, jest prawdziwym wyzwaniem. Dlatego też, inwestują w zaawansowane technologie, które mają zapewnić klienta, że ich dane są chronione przed kradzieżą, lub innym oszustwem. Nietrudno bowiem domyśleć się, jaki wpływ na znane marki ma negatywna prasa.

Jak wygląda mechanizm eksplorowania i jak przebiega atak?

I tak dochodzimy do swoistego wyścigu zbrojeń. Ewoluują nie tylko technologie defensywne. Do nowych zabezpieczeń z łatwością adaptują się Cyberprzestępcy i równie szybko są w stanie przełamać zabezpieczenia.

Zgodnie z ostatnim raportem *Verizon'a* - 8% globalnych przypadków włamań, dotyczy sieci handlowych, a 35% dotyczy szeroko rozumianego sektora finansowego.

Dane kart płatniczych, są cennym aktywem i mogą być szybko spieniężone. Okresy wzmożonego ruchu (przedświąteczne zakupy), zachęcają atakujących do zainwestowania w nowatorskie narzędzia, ponieważ inwestycja szybko się zwraca.

FireEve odkrył, że najczęstszym wektorem ataków, może być: spear phishing, drive-be downloads, oraz SQL Injection, dzięki czemu atakujący wnika do dostawcy usług (np.: aplikacji, poczty, itp.) tworząc tunel VPN, pomiędzy siecią dostawcy a siecią handlową.

Efektem tego działania jest zhakowany kontroler domeny, który zapewnia autoryzację dla kas w punktach sprzedaży detalicznej. Następnie malware, który zbiera dane kart, jest dystrybuowany do kas i przeszukuje aplikacje sprzedażowe, celem zgromadzenia informacji z paska magnetycznego karty, aby wygenerować podróbki.

Innymi słowy, docelowo chodzi o to, aby: zduplikować kartę płatniczą, z którą można przyjść do sklepu, odsprzedać informacje na „czarnym rynku" większemu graczowi, albo samemu (jeśli jest się potężnym), na masową skalę okradać firmy z danych swoich klientów, a transferu pieniędzy dokonywać głównie drogą elektroniczną.

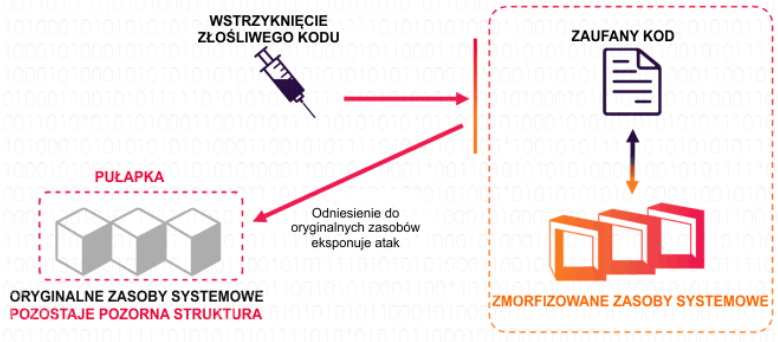
Rady, które kierujemy do właściciela sieci:

1. Zabezpiecz końcowe elementy. Zadbaj o nowsze, lekkie i bardziej dopasowane systemy bezpieczeństwa, czyli: whitelisting, antywirus, antymalware.

Skoro największym zagrożeniem są ataki kierowane i ataki in-memory, możesz–zapomnieć o klasycznej detekcji opartej na sygnaturach.

Pozostają zatem nowoczesne rozwiązania prewencyjne, takie jak MORPHISEC, które zrywają z powszechnymi regułami działania, stawiając przede wszystkim na prewencję.

MORPHISEC zapewnia wydajne oprogramowanie organizacjom zmagającym się z zaawansowanymi zagrożeniami takimi jak zero-day, exploity, itp. Zapobiega zagrożeniom w elementach końcowych, wykorzystując technologię ruchomego celu. Skutecznie ukrywa luki w zabezpieczeniach aplikacji i przeglądarek internetowych.



2. Zadbaj o cykliczne, profesjonalne szkolenie pracowników, połączone z aranżowaniem potencjalnie niebezpiecznych (czyt: mogących narazić firmę na straty) sytuacji. Nie chodzi tu bynajmniej o prowokację, mającą obnażyć czyjąś niekompetencję. Chodzi raczej o wyrobienie odpowiednich nawyków w sytuacjach kryzysowych, o wypracowanie „szlaków komunikacyjnych", a docelowo o wyeliminowanie stereotypowego myślenia: „ - To nie moja sprawa."

Sugerujemy, aby budowanie świadomości odbywało się już na poziomie stażysty. Idealne byłoby dwu-stopniowe szkolenie, łączące teorię z praktyką, obowiązkowo zakończone testem.

3. Zaszyfruj dane posiadanych kart. Rozważ rozwiązanie szyfrowania asymetrycznego „end-to-end", które zaczyna się już od PIN-pada. Zadbaj o to, aby bezpieczeństwo zaczynało się na poziomie „palca klienta", a nie na serwerze.

4. Zainstaluj aktywny monitoring. Szukaj nienormalnych aktywności, podejrzanych logowań, tworzenia dziwnych/niepasujących plików.

5. Segmentuj swoją sieć. Odseparuj system przechowywania danych z kart płatniczych, od reszty środowiska korporacyjnego i koniecznie wymagaj dwu-etapowej identyfikacji przy dostępie do tych danych.

Podsumowanie.

Jeśli mimo wszystko do tej pory, nie przekonały Was powyższe argumenty, albo uważacie, że taki przypadek nie będzie dotyczył Waszej firmy, pozwolę sobie przytoczyć kilka typowych konsekwencji, które być może zmienią dotychczasową optykę i spojrzycie na problem z innej, dalszej perspektywy.

Szacunkowe dane, dla globalnego rynku sprzedaży detalicznej, za rok 2015:

- <u>finansowe:</u>
  - koszty usunięcia skutków włamań (blokady, wirusy, itp.): 300 mln. $
  - skrajne przypadki spadku wartości akcji: 8%
  - spadek zysków w wymiarze rocznym: 46%
  - przychody hakerów zw. tylko z kradzieżą kart płatniczych: 53,7 mln. $ (ok. 2 mln. kart)

- <u>wizerunkowe:</u>
  - spadek reputacji (skargi, procesy, itp.)
  - spadek zaufania klientów (przywiązanie do marki)
  - wymuszone zmiany kadrowe
  - zwiększenie kontroli ze strony „regulatorów rynku”

Jak widać, koszty włamań i długodystansowy wpływ na Twoją firmę, mogą być bolesne!