Kraków, 3.03.23

Analiza zagrożeń dla prywatności w systemach informatycznych

Julia Sadecka, Jakub Augustyn, Beniamin Jankowski

Wyciek danych kart kredytowych klientów *Home Depot*.

1. Charakterystyka zdarzenia

Home Depot jest przedsiębiorstwem, które jest właścicielem sieci hipermarketów The Home Depot w którym sprzedawane, a także wypożyczane są materiały budowlane i narzędzia. Firma ma siedzibę w Atlancie.

W 2014 roku 8 września firma Home Depot wyznała, że doszło do włamania do systemu płatności kartami kredytowymi. Wg firmy śledztwo w tej sprawie rozpoczęło się 6 dni przed przekazaniem informacji klientom dot. włamania.

Charakter tego włamania był zewnętrzny gdyż, był to jeden z wielu ataków na tego typu sklepy - m. in. atak na UPS store kilka miesięca przed atakiem na Home Depot czy atak na Dairy Queen miesiąc po zdarzeniu.

Same włamanie określa się jako przypadek *Memory Scraping Malware*. Atak ten polega na sczytaniu pamięci RAM na terminalach płatniczych poprzez odpowiednio wcześniej napisany szkodliwy program (malware). Program wydobywa interesujące dane dzięki wyrażeniom regularnym, a następnie przesyła je do atakującego. Aby dostać się do sieci terminali hakerzy użyli *podatności zero-day* dla Windowsa.

Dzięki temu, uzyskano nieautoryzowany dostęp do ponad ***7 500*** *samoobsługowych terminali*. Samo włamanie nie zostało odkryte bezpośrednio przez firmę. Wiele banków odkryło, że dane kart kredytowych

znaczącej liczby ich klientów zostały wystawione na sprzedaż na darknecie. Po sprawdzeniu okazało się, że wszystkie te karty były niedawno używane właśnie w sklepach Home Depot. Sam atak często był łączony ze zdarzeniem na naruszenie danych Targetu w 2013 r.

2. Skala i zakres danych

Skradziono około:

- **56 milionów** informacji o kartach kredytowych i debetowych klientów Home Depot.
- **53 miliony** adresów e-mail.

3. Skutki wycieku danych

Dla klientów:

- Sprzedaż ich danych m.in. numerów kart kredytowych na darknecie
- Potrzeba wymiany kart kredytowych, a także adresów email w celu zabezpieczenia ich.

Dla firmy:

- Długoletnie dochodzenia i sprawy sądowe w sprawie naruszenia bezpieczeństwa
- Ponad 263 milionowe koszty związane z naruszeniem prywatności (w koszty wchodzą m.in. koszty prawne, koszty ugody sądowej, koszty związane z wprowadzaniem ulepszeń w systemie bezpieczeństwa, 19.5 mln dolarów wypłacone jako odszkodowania dla klientów, 134.5 mln wypłacone firmom obsługującym karty kredytowe i bankom)
- Uszczerbek na reputacji firmy. Tym samym utrata klientów, którzy przenoszą swoją działalność do innych firm.

Globalne:

- Przez skalę wycieku danych firmy przyłożyły większy nacisk na ochronę informacji swoich klientów. Zmieniono m.in. czytniki kart w sklepach, a także zwrócono większą uwagę na oprogramowania przechowujące dane klientów.
- Klienci zaczęli stosować dodatkowe środki ostrożności w zakresie swoich danych osobowych. Zwiększyła się świadomość zagrożenia idącego z kradzieżą tożsamości.

4. Działania naprawcze

Z wyżej wymienionego incydentu należy wyciągnąć poważne wnioski. Pierwszym elementem było zatrudnienie osoby na stanowisku CISO (*ang. chief information security officer*) oraz przeszkolenie pracowników pod kątem wiedzy związanej z cyberbezpieczeństwem. Był to wielki krok naprzód w ww. firmie.

Oprócz tego wzmocniona została polityka haseł, zostało wprowadzone dwustopniowe uwierzytelnianie, zwiększona została częstość wykonywania testów penetracyjnych.

Definitywnie słabym punktem był też sam system operacyjny w środowisku funkcjonowania POS-ów (*ang. Point Of Sale*) - aplikacji używanych do rejestrowania transakcji. Funkcjonowały one na maszynach z systemem Windows Embedded XP, podczas gdy na rynku były już wersje Windows 7 oraz 8. Używanie starszego systemu naraża użytkownika na mniejszą ilość aktualizacji i wsparcia, w tym aktualizowania bazy danych wirusów malware - który grał kluczową rolę w ataku na Home Depot.
W związku z powyższym należało natychmiast wymienić aplikacje POS na najnowsze modele, operujące w nowym systemie i z nowym, dobrze zaktualizowanym antywirusem.

Zaleceniem też jest używanie płatności typu *peer-to-peer* (P2P), podczas których dane karty nie są wysyłane wraz z środkami. Wymaga to dodatkowej autoryzacji ze strony użytkownika np. przez urządzenie mobilne, w związku z czym znacznie zwiększa bezpieczeństwo przesyłanych środków oraz nie ujawnia danych karty kredytowej.

Bibliografia:
https://sansorg.egnyte.com/dl/d82dKCwimy
https://bestcompany.com/identity-theft/blog/a-look-back-at-the-home-depot-data-breach
https://ir.homedepot.com/news-releases/2014/11-06-2014-014517315
https://duo.com/decipher/home-depot-settles-with-states-over-2014-data-breach