Odzyskiwanie po naruszeniu bezpieczeństwa

Odkryłeś, że doszło do naruszenia bezpieczeństwa danych. Co teraz? Przeczytaj ten rozdział, w którym omówiono, jak reagować w tego typu sytuacjach.

Uncja prewencji jest warta wielu ton odpowiedzi

Jeśli chodzi o usuwanie skutków naruszenia bezpieczeństwa, po prostu nic nie zastąpi odpowiedniego przygotowania. Żadna liczba działań eksperckich po naruszeniu nigdy nie zapewni takiego samego poziomu ochrony, jak właściwe zapobieganie przed włamaniem. Jeśli zastosujesz się do różnych technik opisanych w tej książce, dotyczących sposobów ochrony zasobów elektronicznych, prawdopodobnie będziesz w znacznie lepszej kondycji, aby odzyskać przytomność po naruszeniu, niż gdybyś tego nie zrobił. Przygotowanie nie tylko pomaga w odzyskaniu, ale także pomaga upewnić się, że możesz wykryć naruszenie. Bez odpowiedniego przygotowania możesz nawet nie być w stanie stwierdzić, że nastąpiło naruszenie, nie mówiąc już o powstrzymaniu ataku i powstrzymaniu go.

Zachowaj spokój i działaj teraz z mądrością

Normalną ludzką reakcją na naruszenie cyberprzestrzeni jest poczucie oburzenia, naruszenia, zdenerwowania i / lub paniki, ale aby właściwie zareagować na naruszenie, musisz myśleć logicznie i jasno oraz działać w sposób uporządkowany. Poświęć chwilę, aby powiedzieć sobie, że wszystko będzie dobrze i że typ ataku, z którym masz do czynienia, jest tym, z którym ludzie i firmy odnoszące największe sukcesy będą musieli sobie poradzić w pewnym momencie (lub w wielu miejscach). Podobnie, nie zachowuj się irracjonalnie. Nie próbuj naprawiać swojego problemu, szukając porady w Google. Wiele osób w Internecie udziela złych porad. Co gorsza, wiele nieuczciwych witryn internetowych z poradami dotyczącymi usuwania złośliwego oprogramowania i zatrzymywania ataków umieszcza złośliwe oprogramowanie na komputerach uzyskujących do nich dostęp! Oczywiście nie pobieraj oprogramowania zabezpieczającego ani niczego innego z podejrzanych witryn. Pamiętaj też, że musisz działać jak najszybciej. Przerwij wszystko, co robisz, i skup się na rozwiązaniu problemu. Zamknij wszystkie programy, których używasz, zapisz (i wykonaj kopię zapasową na nośnikach, które przeskanujesz w poszukiwaniu złośliwego oprogramowania przed ponownym użyciem), wszystkie otwarte dokumenty i tak dalej, i zabierz się do pracy nad odzyskaniem po naruszeniu. Kiedy dojdzie do naruszenia, czas działa na Twoją niekorzyść. Im szybciej powstrzymasz kogoś przed kradzieżą plików, uszkodzeniem danych lub atakowaniem dodatkowych urządzeń w sieci, tym lepiej będzie.

Znajdź profesjonalistę

Najlepiej byłoby zatrudnić specjalistę ds. cyberbezpieczeństwa, który pomoże Ci odzyskać zdrowie. Chociaż ta książka zawiera dobre wskazówki, jeśli chodzi o umiejętności techniczne, nic nie zastąpi wieloletniego doświadczenia dobrego profesjonalisty. Powinieneś zastosować tę samą logikę i szukać profesjonalnej pomocy w obliczu poważnego kryzysu związanego z komputerem i danymi, jak gdybyś spełniał którykolwiek z poniższych warunków:

* Jeśli byłeś poważnie chory, udałeś się do lekarza lub szpitala.

* Jeśli zostałeś aresztowany i oskarżony o popełnienie przestępstwa, zatrudniłbyś prawnika.

* Jeśli urząd skarbowy wysłał Ci pismo, że przechodzisz audyt, powinieneś zatrudnić księgowego

Wychodzenie z naruszenia bez pomocy profesjonalisty

Jeśli nie masz możliwości sprowadzenia specjalisty, wykonaj następujące czynności. Te kroki są zasadniczo tymi, których przestrzega większość profesjonalistów:

1. Dowiedz się, co się stało (lub się dzieje).

2. Powstrzymaj atak.

3. Przerwij i wyeliminuj atak.

Krok 1: Dowiedz się, co się stało lub się dzieje

Jeśli to możliwe, chcesz dowiedzieć się jak najwięcej o ataku, aby móc odpowiednio zareagować. Jeśli osoba atakująca przenosi pliki z komputera na inne urządzenie, na przykład chcesz jak najszybciej odłączyć swoje urządzenie od Internetu. To powiedziawszy, większość użytkowników domowych nie ma umiejętności technicznych, aby właściwie przeanalizować i dokładnie zrozumieć, jaki może być charakter danego ataku - chyba że, oczywiście, atak ma charakter jawny.

GDY ATAK JEST NIEWYKRYTY

Brak wiedzy w tej dziedzinie przez przeciętnego człowieka nie powinien dziwić. Większość firm, które zostały naruszone, w tym wiele z własnymi pracownikami zajmującymi się bezpieczeństwem informacji, nawet nie odkrywa, że zostały one skutecznie naruszone, aż do miesięcy po rozpoczęciu ataku przez osoby atakujące! Niektórzy eksperci szacują, że firmy średnio nie wykrywają jawnych naruszeń bezpieczeństwa informacji, dopóki nie upłynie od sześciu miesięcy do roku od momentu wystąpienia pierwszego naruszenia!

Zbierz jak najwięcej informacji na temat

*Co się stało

* Jakie systemy informacyjne i bazy danych zostały trafione

* Co może zrobić przestępca lub inna złośliwa strona ze skradzionym materiałem

* Jakie dane i programy zostały naruszone

* Kto, oprócz Ciebie, może być narażony na ryzyko z powodu naruszenia (obejmuje to wszelkie potencjalne konsekwencje dla Twojego pracodawcy)

Nie spędzaj dużo czasu na tym kroku - musisz podjąć działania, a nie tylko udokumentować - ale im więcej masz informacji, tym większe są szanse, że będziesz w stanie zapobiec kolejnemu podobnemu atakowi w przyszłości.

Krok 2: Powstrzymaj atak

Odetnij napastnika, izolując go od zainfekowanych urządzeń. Zawarcie może wiązać się z:

* Kończenie wszystkich połączeń sieciowych JAK NAJSZYBCIEJ: Aby zakończyć łączność sieciową dla wszystkich urządzeń w sieci, wyłącz router, odłączając go. (Uwaga: jeśli prowadzisz działalność biznesową, ten krok zwykle nie jest możliwy).

* Odłączanie wszelkich kabli Ethernet: pamiętaj jednak, że atak sieciowy mógł już rozprzestrzenić się na inne urządzenia w sieci. Jeśli tak, odłącz sieć od Internetu i odłącz każde urządzenie od sieci, aż zostanie przeskanowane pod kątem problemów z bezpieczeństwem.

* Wyłączanie Wi-Fi na zainfekowanym urządzeniu: Ponownie, atak sieciowy mógł już rozprzestrzenić się na inne urządzenia w sieci. Jeśli tak, odłącz sieć od Internetu i odłącz każde urządzenie od sieci, wyłączając Wi-Fi na routerze i wszelkich punktach dostępu, a nie tylko na zainfekowanym komputerze.

* Wyłączanie danych komórkowych: Innymi słowy, przełącz urządzenie w tryb samolotowy.

* Wyłączanie Bluetooth i NFC: Bluetooth i NFC to technologie komunikacji bezprzewodowej, które działają z urządzeniami znajdującymi się blisko siebie. Wszelka taka komunikacja powinna być blokowana, jeśli istnieje możliwość rozprzestrzeniania się infekcji lub hakerów przeskakujących z urządzenia na urządzenie.

* Odłączanie dysków USB i innych dysków wymiennych od systemu: Uwaga: dyski mogą zawierać złośliwe oprogramowanie, więc nie należy podłączać ich do żadnych innych systemów.

* Odwołanie wszelkich praw dostępu wykorzystywanych przez atakującego: jeśli masz udostępnione urządzenie, a osoba atakująca korzysta z konta innego niż Twoje, do którego w jakiś sposób uzyskał autoryzowany dostęp, tymczasowo ustaw to konto tak, aby nie miało żadnych uprawnień.

ZAKOŃCZENIE ŁĄCZNOŚCI SIECIOWEJ

Chociaż możesz rozłączyć połączenie internetowe, fizycznie odłączając je od routera lub połączenia sieciowego, możesz również wyłączyć połączenie na swoich urządzeniach. Aby zakończyć łączność sieciową na komputerze z systemem Windows, wykonaj następujące kroki:

1. Wybierz Ustawienia ⇒ Połączenia sieciowe.

2. Kliknij prawym przyciskiem myszy odpowiednie połączenie (lub połączenia pojedynczo), a następnie kliknij opcję Wyłącz.

Jeśli z jakiegoś powodu potrzebujesz dostępu do Internetu z urządzenia, aby uzyskać pomoc w jego wyczyszczeniu, wyłącz wszystkie inne urządzenia w sieci, aby zapobiec rozprzestrzenianiu się ataków z sieci na urządzenie. Należy pamiętać, że taki scenariusz jest daleki od ideału. Chcesz odciąć zainfekowane urządzenie od reszty świata, a nie tylko przerwać połączenia między nim a innymi urządzeniami.

Krok 3: Przerwij i wyeliminuj atak

Zawarcie ataku to nie to samo, co przerywanie i eliminowanie ataku. Złośliwe oprogramowanie, które było obecne na zainfekowanym urządzeniu, jest nadal obecne po odłączeniu urządzenia od Internetu, na przykład, podobnie jak wszelkie luki w zabezpieczeniach, które zdalny potwierdzający lub złośliwe oprogramowanie mogło wykorzystać, aby przejąć kontrolę nad urządzeniem. Dlatego po powstrzymaniu ataku ważne jest, aby oczyścić system. W poniższych sekcjach opisano niektóre kroki, które należy wykonać w tym momencie

Uruchom komputer z dysku rozruchowego oprogramowania zabezpieczającego

Jeśli masz dysk rozruchowy oprogramowania zabezpieczającego, uruchom z niego. Większość współczesnych użytkowników nie będzie miała takiego dysku. Jeśli nie, przejdź do następnej sekcji.

1. Usuń wszystkie napędy USB, DVD, CD, dyskietki (tak, niektórzy nadal je mają) i wszelkie inne zewnętrzne napędy z komputera.

2. Włóż dyskietkę startową do napędu CD / DVD.

3. Wyłącz komputer.

4. Poczekaj dziesięć sekund i naciśnij przycisk zasilania, aby uruchomić komputer.

5. Jeśli używasz komputera z systemem Windows i nie uruchamia się on z dysku CD, wyłącz urządzenie, odczekaj dziesięć sekund i uruchom go ponownie, naciskając przycisk rozruchu systemu BIOS (różne

komputery używają różnych przycisków, ale większość używa niektórych przycisków F- klawisz F1 lub F2), aby przejść do ustawień BIOS-u i ustawić go tak, aby uruchamiał się z dysku CD, jeśli jest obecny, przed próbą uruchomienia z dysku twardego.

6. Wyjdź z systemu BIOS i uruchom ponownie.

Jeśli używasz komputera z systemem Windows, uruchom komputer w trybie awaryjnym. Tryb awaryjny to specjalny tryb systemu Windows, który umożliwia uruchamianie tylko niezbędnych usług systemowych i programów podczas uruchamiania systemu. Aby to zrobić, wykonaj następujące kroki:

1. Usuń wszystkie napędy USB, DVD, CD, dyskietki (tak, niektórzy nadal je mają) i wszelkie inne zewnętrzne napędy z komputera.

2. Wyłącz komputer.

3. Poczekaj dziesięć sekund i naciśnij przycisk zasilania, aby uruchomić komputer.

4. Podczas uruchamiania komputera naciśnij kilkakrotnie klawisz F8, aby wyświetlić menu opcji rozruchu.

5. Gdy pojawi się menu Boot Options, wybierz opcję uruchamiania w trybie awaryjnym.

Jeśli używasz Maca, uruchom go za pomocą Bezpiecznego rozruchu. MacOS nie zapewnia pełnego odpowiednika trybu awaryjnego. Komputery Mac zawsze uruchamiają się z włączoną obsługą sieci. Jego Bezpieczny rozruch jest czystszy niż normalny rozruch. Aby wykonać bezpieczny rozruch, wykonaj następujące kroki:

1. Usuń wszystkie napędy USB, DVD, CD, dyskietki (tak, niektórzy nadal je mają) i wszelkie inne zewnętrzne napędy z komputera.

2. Wyłącz komputer.

3. Poczekaj dziesięć sekund i naciśnij przycisk zasilania, aby uruchomić komputer.

4. Podczas uruchamiania komputera przytrzymaj klawisz Shift.

Starsze komputery Mac (wersje macOS 6–9) uruchamiają się w specjalnym trybie administratora bez rozszerzeń, jeśli użytkownik naciśnie klawisz wstrzymania podczas ponownego uruchamiania. Porada dotycząca rozruchu za pomocą Bezpiecznego rozruchu dotyczy tylko komputerów Mac, na których działają częściej najnowsze systemy operacyjne.

Utworzyć kopię zapasową

Miejmy nadzieję, że możesz zignorować tę sekcję, ponieważ zwróciłeś uwagę na porady zawarte w części o kopiach zapasowych, ale jeśli ostatnio nie tworzyłeś kopii zapasowych danych, zrób to teraz. Oczywiście utworzenie kopii zapasowej zagrożonego urządzenia niekoniecznie spowoduje zapisanie wszystkich danych (ponieważ niektóre mogą być już uszkodzone lub brakujące), ale jeśli nie masz jeszcze kopii zapasowej, zrób to teraz - najlepiej, kopiując pliki na zewnętrzny Dysk USB, którego nie podłączysz do żadnych innych urządzeń, dopóki nie zostanie prawidłowo przeskanowany przez oprogramowanie zabezpieczające.

Usuń śmieci (opcjonalnie)

W tym momencie możesz chcieć usunąć wszystkie pliki, których nie potrzebujesz, w tym te tymczasowe, które w jakiś sposób stały się trwałe (lista takich plików znajduje się w rozdziale o kopiach zapasowych).

Dlaczego teraz usunąć?

Cóż, powinieneś przeprowadzać okresową konserwację, a jeśli teraz czyścisz komputer, teraz jest dobry moment. Im mniej oprogramowania zabezpieczającego może skanować i analizować, tym szybciej będzie działać. Ponadto niektóre złośliwe oprogramowanie ukrywa się w plikach tymczasowych, więc usunięcie takich plików może również bezpośrednio usunąć niektóre złośliwe oprogramowanie. W przypadku użytkowników komputerów z systemem Windows jednym prostym sposobem usunięcia plików tymczasowych jest użycie wbudowanego narzędzia Oczyszczanie dysku:

1. W systemie Windows 10 w polu wyszukiwania na pasku zadań wpisz czyszczenie dysku.

2. Wybierz Oczyszczanie dysku z listy wyników

3. Wybierz dysk, który chcesz wyczyścić, a następnie kliknij OK.

4. Wybierz typy plików, których chcesz się pozbyć, a następnie kliknij OK.

5. Kliknij Akcesoria (lub Akcesoria Windows).

6. Kliknij Oczyszczanie dysku.

Uruchom oprogramowanie zabezpieczające

Mamy nadzieję, że masz już zainstalowane oprogramowanie zabezpieczające. Jeśli tak, uruchom pełne skanowanie systemu. Jedno ważne zastrzeżenie: oprogramowanie zabezpieczające działające na zaatakowanym urządzeniu samo może być zagrożone lub bezsilne wobec danego zagrożenia (w końcu naruszenie bezpieczeństwa miało miejsce przy uruchomionym oprogramowaniu zabezpieczającym), więc niezależnie od tego, czy takie skanowanie zakończy się pomyślnie, rozsądnym rozwiązaniem może być uruchomienie oprogramowania zabezpieczającego z rozruchowego dysku CD lub innego nośnika tylko do odczytu lub, w przypadku niektórych produktów, z innego komputera w sieci domowej. Nie wszystkie marki oprogramowania zabezpieczającego wychwytują wszystkie warianty złośliwego oprogramowania. Specjaliści ds. Bezpieczeństwa wykonujący „czyszczenie" urządzenia często używają oprogramowania zabezpieczającego od wielu dostawców. Jeśli używasz komputera Mac, a Bezpieczny rozruch obejmuje dostęp do Internetu, uruchom procedury aktualizacji oprogramowania zabezpieczającego przed uruchomieniem pełnego skanowania. Złośliwe oprogramowanie lub osoby atakujące mogą dodawać nowe pliki do systemu, usuwać pliki i modyfikować pliki. Mogą również otwierać porty komunikacyjne. Oprogramowanie zabezpieczające powinno być w stanie sprostać wszystkim tym scenariuszom. Zwróć uwagę na raporty generowane przez oprogramowanie zabezpieczające po jego uruchomieniu. Śledź dokładnie, co usunął lub naprawił. Ta informacja może być ważna, jeśli na przykład niektóre programy nie działają po czyszczeniu. (Konieczne może być ponowne zainstalowanie programów, z których usunięto pliki lub z których usunięto złośliwe oprogramowanie w plikach zmodyfikowanych przez złośliwe oprogramowanie). Bazy danych poczty e-mail mogą wymagać przywrócenia, jeśli w wiadomościach znaleziono złośliwe oprogramowanie, a oprogramowanie zabezpieczające nie mogło w pełni usunąć bałaganu. Informacje z raportu oprogramowania zabezpieczającego mogą być również przydatne dla specjalisty ds. Cyberbezpieczeństwa lub informatyka, jeśli zatrudnisz go później. Ponadto informacje zawarte w raporcie mogą dostarczyć wskazówek, gdzie atak się rozpoczął i co umożliwiło jego wystąpienie, pomagając tym samym w zapobieganiu jego ponownemu wystąpieniu.

Oprogramowanie zabezpieczające często wykrywa i zgłasza różne materiały nie będące atakami, które mogą być niepożądane ze względu na ich wpływ na prywatność lub możliwość nakłonienia użytkownika za pomocą reklam. Możesz na przykład zobaczyć alerty, że oprogramowanie zabezpieczające wykryło

śledzące pliki cookie lub oprogramowanie reklamowe; nie jest też poważnym problemem, ale możesz chcieć usunąć adware, jeśli przeszkadzają Ci one. W wielu przypadkach można zapłacić za uaktualnienie oprogramowania wyświetlającego reklamy do wersji płatnej, w której brakuje reklam. Jeśli chodzi o regenerację po ataku, te niepożądane elementy nie stanowią problemu. Czasami oprogramowanie zabezpieczające poinformuje Cię, że musisz uruchomić dodatek, aby w pełni wyczyścić system. Na przykład firma Symantec oferuje narzędzie Norton Power Eraser, o którym mówi: „Eliminuje głęboko osadzone i trudne do wykrycia oprogramowanie przestępcze, którego nie zawsze wykrywa tradycyjne skanowanie wirusów". Jeśli Twoje oprogramowanie zabezpieczające informuje Cię, że musisz uruchomić taki skaner, powinieneś to zrobić, ale upewnij się, że uzyskasz go z legalnego, oficjalnego, oryginalnego źródła. Ponadto nigdy nie pobieraj ani nie uruchamiaj żadnego skanera tego rodzaju, jeśli zostaniesz o to poproszony w wyniku działania oprogramowania zabezpieczającego. Wiele fałszywych wyskakujących okienek doradzi Ci podobnie, ale zainstaluj złośliwe oprogramowanie, pobierz odpowiednie „oprogramowanie zabezpieczające".

Zainstaluj ponownie uszkodzone oprogramowanie

Są eksperci, którzy zalecają odinstalowanie i ponowne zainstalowanie dowolnego pakietu oprogramowania, o którym wiesz, że został dotknięty atakiem, nawet jeśli oprogramowanie zabezpieczające go naprawiło.

Uruchom ponownie system i uruchom zaktualizowane skanowanie bezpieczeństwa

W przypadku komputerów z systemem Windows, po wyczyszczeniu systemu, uruchom go ponownie w trybie awaryjnym z obsługą sieci, korzystając z procedury opisanej powyżej (ale wybierając tryb awaryjny z obsługą sieci zamiast trybu awaryjnego), uruchom oprogramowanie zabezpieczające, pobierz wszystkie aktualizacje i uruchom oprogramowanie zabezpieczające przeskanuj ponownie. Jeśli nie ma aktualizacji, nie ma potrzeby ponownego uruchamiania oprogramowania zabezpieczającego. Jeśli używasz komputera Mac, Bezpieczny rozruch zawiera już obsługę sieci, więc nie ma powodu, aby powtarzać skanowanie. Zainstaluj wszystkie odpowiednie aktualizacje i poprawki. Jeśli którekolwiek z Twoich programów nie zostało zaktualizowane do najnowszej wersji i może zawierać luki, napraw to podczas czyszczenia. Jeśli masz na to czas, po zainstalowaniu wszystkich aktualizacji uruchom ponownie pełne skanowanie oprogramowania zabezpieczającego. Istnieje kilka powodów, dla których warto to zrobić, w tym fakt, że chcesz, aby sprawdzał system przy użyciu własnych najbardziej aktualnych informacji o złośliwym oprogramowaniu i innych zagrożeniach, a także fakt, że chcesz, aby jego silnik analizy heurystycznej miał podstawowe informacje o tym, jak system wygląda z najnowszymi aktualizacjami.

Usuń wszystkie potencjalnie problematyczne punkty przywracania systemu

Przywracanie systemu to przydatne narzędzie, ale może być również niebezpieczne. Jeśli na przykład system tworzy punkt przywracania, gdy na urządzeniu działa złośliwe oprogramowanie, przywrócenie do tego punktu prawdopodobnie przywróci złośliwe oprogramowanie! Dlatego po wyczyszczeniu systemu pamiętaj, aby usunąć wszystkie punkty przywracania systemu, które mogły zostać utworzone, gdy system został naruszony. Jeśli nie masz pewności, czy punkt przywracania może być problematyczny, usuń go. W przypadku większości użytkowników oznacza to, że warto usunąć wszystkie punkty przywracania systemu. Aby to zrobić:

1. Kliknij menu Start.

2. Kliknij Panel sterowania.

3. Kliknij Wszystkie elementy panelu sterowania.

4. Kliknij Odzyskiwanie.

5. Kliknij Konfiguruj przywracanie systemu.

6. Postępuj zgodnie z wyświetlanymi instrukcjami, aby usunąć odpowiednie punkty przywracania systemu.

Przywracanie zmodyfikowanych ustawień

Niektórzy atakujący i złośliwe oprogramowanie mogą modyfikować różne ustawienia na Twoim urządzeniu. Strona, którą widzisz po uruchomieniu przeglądarki internetowej - na przykład strona główna przeglądarki - jest jednym z typowych elementów, które złośliwe oprogramowanie często zmienia. Zmiana strony przeglądarki z powrotem na bezpieczną jest ważna, ponieważ strona początkowa złośliwego oprogramowania może prowadzić do strony, która ponownie instaluje złośliwe oprogramowanie lub wykonuje inne nikczemne zadanie.

Poniższe sekcje przeprowadzą Cię przez proces dla każdej przeglądarki. W przypadku korzystania z przeglądarek w wersji na telefon lub tablet, opisanych w kolejnych rozdziałach, proces będzie się nieco różnić, ale powinien być po prostu rozpoznawalny na podstawie instrukcji.

W CHROMIE

Aby zresetować przeglądarkę Chrome:

1. Kliknij ikonę menu z trzema kropkami w prawym górnym rogu.

2. Kliknij Ustawienia.

3. Przewiń w dół do sekcji Przy uruchomieniu i odpowiednio ją skonfiguruj.

W FIREFOX

Aby zresetować przeglądarkę Firefox:

1. Kliknij ikonę menu z trzema liniami w prawym górnym rogu.

2. Kliknij Opcje.

3. Kliknij Strona główna.

4. Skonfiguruj odpowiednio wartości w sekcji Nowe okna i karty.

W SAFARI

Aby zresetować przeglądarkę Safari:

1. Kliknij menu Safari.

2. Kliknij Preferencje.

3. Kliknij kartę Ogólne.

4. Przewiń w dół do pola Strona główna i odpowiednio je skonfiguruj.

W EDGE

Aby zresetować przeglądarkę Edge:

Aby zresetować przeglądarkę Edge:

1. Kliknij ikonę menu z trzema kropkami w prawym górnym rogu.

2. Kliknij Ustawienia.

3. Skonfiguruj Open Microsoft Edge za pomocą i Otwórz nowe karty z odpowiednimi sekcjami.

Odbuduj system

Czasami łatwiej, zamiast postępować zgodnie z powyższymi procesami, jest po prostu przebudować system od podstaw. W rzeczywistości, ze względu na ryzyko pominięcia jakiegoś problemu przez oprogramowanie zabezpieczające lub pomyłki użytkowników podczas czyszczenia zabezpieczeń, wielu ekspertów zaleca, aby zawsze, gdy jest to możliwe, całkowicie przebudować system po naruszeniu. Nawet jeśli planujesz odbudować system w odpowiedzi na naruszenie, rozsądnie jest przeprowadzić skanowanie oprogramowania zabezpieczającego przed wykonaniem tego zadania, ponieważ istnieją rzadkie formy złośliwego oprogramowania, które mogą przetrwać nawet po przywróceniu (na przykład złośliwe oprogramowanie przeprogramowujące BIOS, niektóre wirusy sektora rozruchowego itd.) oraz skanowanie wszystkich urządzeń w tej samej sieci, w której znajduje się zagrożone urządzenie w momencie naruszenia zabezpieczeń lub później, aby upewnić się, że nic złego nie może rozprzestrzenić się z powrotem na nowo przywrócone urządzenie.

Postępowanie ze skradzionymi informacjami

Jeśli włamano się do komputera, telefonu lub tabletu, jest to możliwe ,że poufne informacje zostały skradzione i mogą zostać wykorzystane przez przestępcę. Należy na przykład zmienić dowolne z haseł przechowywanych na urządzeniu i sprawdzić wszystkie konta, do których można było uzyskać dostęp z urządzenia bez logowania (ze względu na wcześniejsze ustawienie urządzenia na „Zapamiętaj mnie" po pomyślnym zalogowaniu), aby upewnij się, że nic nie pójdzie źle. Oczywiście, jeśli Twoje hasła były przechowywane w mocno zaszyfrowanym formacie, potrzeba ich zmiany jest mniej pilna, niż gdyby były przechowywane w postaci zwykłego tekstu lub ze słabym szyfrowaniem, ale najlepiej, jeśli nie masz pewności, że szyfrowanie wytrzyma długo termin, i tak powinieneś je zmienić. Jeśli podejrzewasz, że mogły zostać pobrane informacje, które mogłyby zostać wykorzystane do podszywania się pod Ciebie, rozsądnie może być również zainicjowanie wstrzymania kredytu i złożenie raportu policyjnego. Zachowaj przy sobie kopię raportu policyjnego. Jeśli zostaniesz zatrzymany przez policjanta, który poinformuje Cię, że istnieje nakaz aresztowania w miejscu, w którym nigdy nie byłeś, na przykład, będziesz mieć dowód, że złożyłeś zgłoszenie, że prywatne informacje, które mogłyby zostać wykorzystane do ukraść twoją tożsamość, została ci skradziona. Taki dokument nie może całkowicie uchronić Cię przed problemami, ale z pewnością może poprawić Twoją sytuację w takim scenariuszu, niż byłoby, gdybyś nie miał takiego dowodu. Jeśli uważasz, że dane Twojej karty kredytowej lub debetowej zostały skradzione, skontaktuj się z odpowiednią stroną pod numerem telefonu wydrukowanym na odwrocie karty, powiedz im, że numer mógł zostać przejęty, i poproś o wydanie nowej karty z nowy numer. Sprawdź również konto pod kątem podejrzanych transakcji. Prowadź rejestr każdego połączenia, które wykonałeś, kiedy je wykonałeś, z kim rozmawiałeś i co się wydarzyło podczas rozmowy. Im bardziej wrażliwe są te informacje, tym ważniejsze jest, aby je zabrać działanie i podjęcie go szybko. Oto kilka sposobów myślenia o informacjach:

* Nie jest prywatny, ale może pomóc przestępcom w kradzieży tożsamości:

-Nazwiska, adres i numer telefonu domowego. Tego typu informacje są naprawdę dostępne dla każdego, kto ich chce, nawet bez hakowania. (Weź pod uwagę, że pokolenie temu tego typu informacje były dosłownie publikowane w książkach telefonicznych i wysyłane do każdego domu, który miał linię telefoniczną). To powiedziawszy, tego typu informacje mogą być używane w połączeniu z innymi

informacjami do popełnienia wszelkiego rodzaju przestępstw, zwłaszcza jeśli niczego nie podejrzewając inne osoby popełniają błędy (na przykład pozwalając osobie posiadającej te informacje na otwarcie karty bibliotecznej bez okazania dokumentów tożsamości) .

-Inne informacje z publicznych rejestrów: cena, jaką zapłaciłeś za swój dom, imiona swoich dzieci i tak dalej. Chociaż te informacje są publicznie dostępne, przestępca zestawiający je z innymi informacjami, które mogą zostać usunięte z komputera, może spowodować problemy.

* Wrażliwe: adresy e-mail, numery telefonów komórkowych, numery kont kart kredytowych bez kodu CVC, numery kont kart debetowych, które wymagają kodu PIN do użycia lub bez kodu CVC, numery kart bankomatowych, numery legitymacji studenckich, numery paszportów, pełne urodziny, w tym rok i tak dalej. Te elementy stwarzają zagrożenie bezpieczeństwa, gdy zostaną przejęte - na przykład skradziony adres e-mail może prowadzić do wyrafinowanych ataków phishingowych, które wykorzystują inne informacje zebrane z komputera, próby włamania się na konto, wiadomości spamowe itp. Tego rodzaju skradzione informacje mogą być również wykorzystywane przez przestępców w ramach kradzieży tożsamości i oszustw finansowych, ale mogą wymagać połączenia wielu informacji w celu stworzenia poważnego ryzyka.

* Bardziej wrażliwe: numery PESEL (lub ich zagraniczne odpowiedniki), hasła do kont internetowych, numery kont bankowych (w przypadku ujawnienia ich przez potencjalnego przestępcę w przeciwieństwie do umieszczania ich na czeku przekazanym zaufanej stronie), PIN-y, karty kredytowe i debetowe informacje z kodem CVC, odpowiedzi na pytania kwestionujące, których używałeś do zabezpieczania kont i tak dalej. Tego typu informacje często mogą być nadużywane samodzielnie.

Płacenie okupu

Jeśli masz odpowiednie kopie zapasowe, możesz usunąć oprogramowanie ransomware w taki sam sposób, jak inne złośliwe oprogramowanie. Jeśli jakiekolwiek dane zostaną utracone w trakcie procesu, możesz je przywrócić z kopii zapasowych. Jeśli zostałeś zaatakowany przez oprogramowanie ransomware i nie masz odpowiednich kopii zapasowych, możesz stanąć przed trudną decyzją. Oczywiście nie leży w Twoim wspólnym interesie zapłacenie okupu przestępcy w celu odzyskania danych, ale w niektórych przypadkach, jeśli Twoje dane są dla Ciebie ważne, może to być droga, którą musisz się udać. W wielu przypadkach przestępcy nawet nie zwrócą Ci danych, jeśli zapłacisz okup - więc płacąc okup, możesz nie tylko zmarnować pieniądze, ale nadal cierpieć na trwałą utratę danych. Będziesz musiał zdecydować, czy chcesz skorzystać z tej szansy. (Miejmy nadzieję, że ten akapit będzie silną motywacją dla czytelników do proaktywnego tworzenia kopii zapasowych, jak to omówiono w rozdziale o kopiach zapasowych). Przed zapłaceniem okupu skonsultuj się z ekspertem ds. Bezpieczeństwa informacji. Niektóre oprogramowanie ransomware można usunąć i cofnąć jego skutki za pomocą różnych narzędzi bezpieczeństwa. Jeśli jednak oprogramowanie zabezpieczające nie powie Ci, że może cofnąć szyfrowanie dokonane przez oprogramowanie ransomware, nie próbuj samodzielnie usuwać oprogramowania ransomware po zaszyfrowaniu danych. Niektóre zaawansowane oprogramowanie ransomware trwale usuwa dane, jeśli wykryje próby odszyfrowania danych. Należy również pamiętać, że niektóre zaawansowane oprogramowanie ransomware nie szyfruje danych, ale raczej usuwa je z urządzenia ofiary i przesyła je z powrotem tylko wtedy, gdy usuwa je z urządzenia ofiary i tylko przesyła. Takie oprogramowanie ransomware może być usuwane przez oprogramowanie zabezpieczające, ale oprogramowanie zabezpieczające zwykle nie może przywrócić danych wykradanych przez oprogramowanie ransomware. Najlepszą ochroną użytkowników domowych przed wpływem oprogramowania ransomware jest tworzenie kopii zapasowych i odłączanie ich od wszystkiego innego!

Nauka na przyszłość

Ważne jest, aby uczyć się na naruszeniach. Jeśli możesz dowiedzieć się, co poszło źle i jak hakerowi udało się dostać do twojego systemu (bezpośrednio lub przy użyciu złośliwego oprogramowania), możesz ustanowić dla siebie de facto zasady i procedury, aby zapobiec takim zagrożeniom w przyszłości. Specjalista ds. Bezpieczeństwa cybernetycznego może Ci w tym pomóc.

Odzyskiwanie danych w przypadku naruszenia bezpieczeństwa danych przez stronę trzecią

Prawie wszyscy internauci otrzymali powiadomienie od firmy lub podmiotu rządowego (lub oba), że dane osobowe zostały potencjalnie zagrożone. To, jak podejmiesz taki scenariusz, zależy od wielu czynników, ale poniższe sekcje przedstawiają podstawowe informacje, które musisz wiedzieć.

Powód wysłania powiadomienia

Wiele rodzajów naruszeń danych prowadzi do wysyłania przez organizacje powiadomień. Jednak nie wszystkie z nich stanowią dla Ciebie ten sam poziom ryzyka. Powiadomienia mogą być wysyłane, gdy firma ma

* Wiedzę, że niezaszyfrowana baza danych zawiera dane osobowe i informacje zostały zdecydowanie skradzione

* Wiedzę, że zaszyfrowana baza danych zawierająca dane osobowe została zdecydowanie skradziona

* Wykrytą nieautoryzowaną aktywność na urządzeniu komputerowym zawierającym Twoje informacje

* Wykrytą nieautoryzowaną aktywność na urządzeniu komputerowym, ale nie na tym, które przechowuje Twoje informacje (ale na jednym podłączonym do tej samej lub logicznie połączonej sieci)

* Wykrytą kradzież numerów kart kredytowych lub debetowych, co może mieć miejsce w przypadku urządzenia do pobierania danych lub włamania do urządzenia przetwarzającego karty kredytowe w punkcie sprzedaży. nośniki pamięci lub informacje w formie papierowej

* Odkryła, że były lub mogły być niewłaściwie rozpowszechniane informacje, takie jak informacje wrażliwe wysłane do niewłaściwych stron, niezaszyfrowana wiadomość e-mail wysłana do upoważnionych stron i tak dalej

We wszystkich tych przypadkach działanie może być uzasadnione. Ale jeśli firma powiadomi Cię, że niezaszyfrowana baza haseł, w tym Twoje, została skradziona, potrzeba działania jest pilniejsza niż w przypadku wykrycia nieautoryzowanej aktywności w systemie w tej samej sieci co inny komputer, zawierającej jedynie zaszyfrowaną wersję Twojego hasła.

Oszustwa

Przestępcy widzą, kiedy naruszenie zwraca szczególną uwagę i często wykorzystuje je do własnych niecnych celów. Jedną z powszechnych technik jest wysyłanie przez oszustów fałszywych wiadomości e-mail podszywających się pod osobę, do której ktoś włamał się. Te e-maile zawierają instrukcje dotyczące konfiguracji monitorowania zdolności kredytowej lub złożenia wniosku o rekompensatę pieniężną za ból i niedogodności poniesione w wyniku naruszenia. Oczywiście odsyłacze w takich wiadomościach prowadzą do witryn wyłudzających informacje, witryn instalujących złośliwe oprogramowanie i innych miejsc docelowych, do których nie chcesz się udawać. Przestępcy również działają szybko. Na przykład w lutym 2015 r. Better Business Bureaus zaczęło zgłaszać skargi dotyczące e-maili podszywających się pod Anthem, Inc., niecały dzień po tym, jak firma ubezpieczeniowa ogłosiła naruszenie.

Hasła

Jednym z rodzajów naruszeń najczęściej zgłaszanych w środkach masowego przekazu jest kradzież baz haseł. Nowoczesne systemy uwierzytelniania haseł mają na celu zapewnienie pewnej ochrony w przypadku naruszenia. Hasła są zwykle przechowywane w postaci zakodowanej, co oznacza, że są przechowywane z szyfrowaniem jednokierunkowym. Kiedy wprowadzasz swoje hasło podczas próby logowania, wpisane hasło jest zaszyfrowane, a następnie porównywane z odpowiednią wartością skrótu przechowywaną w bazie danych haseł. W związku z tym Twoje rzeczywiste hasło nie jest nigdzie przechowywane i nie ma go w bazie danych haseł. Jeśli więc haker wykradnie bazę danych haseł, nie otrzyma go natychmiast. Przynajmniej tak to powinno działać. W rzeczywistości jednak nie wszystkie systemy uwierzytelniania są zaimplementowane doskonale; Zaszyfrowane bazy danych haseł mają wiele możliwych do wykorzystania słabych punktów, z których niektóre mogą pomóc przestępcom w rozszyfrowaniu haseł, nawet gdy są one zaszyfrowane. Na przykład, jeśli przestępca przegląda bazę danych i widzi, że zaszyfrowane hasło dla wielu osób jest takie samo, prawdopodobnie będzie to wspólne hasło (może nawet „hasło"), które często można szybko złamać. Istnieją zabezpieczenia przed takimi atakami, ale wiele systemów uwierzytelniania ich nie używa. W związku z tym, jeśli firma powiadomi Cię, że zostało naruszone i że została skradziona zaszyfrowana wersja Twojego hasła, prawdopodobnie powinieneś zresetować hasło. Nie musisz jednak panikować. W większości przypadków Twoje hasło było prawdopodobnie chronione przez haszowanie (chyba że wybrałeś wspólne, słabe hasło, którego oczywiście nie powinieneś mieć). Jeśli z jakiegoś powodu ponownie wykorzystałeś złamane hasło w innych witrynach, na których nie chcesz, aby nieupoważnione osoby logowały się jako Ty, powinieneś zresetować swoje hasło i tym razem nie używaj ponownie nowego hasła!

Informacje o karcie płatniczej

Jeśli dane karty kredytowej lub dane karty debetowej mogły zostać przejęte, podejmij następujące kroki:

* Wykorzystaj usługi monitorowania kredytów. Firmy, do których doszło do naruszenia, często dają osobom potencjalnie dotkniętym przez dane naruszenia bezpłatny rok lub dwa na monitorowanie kredytu. Chociaż nigdy nie należy polegać na takich usługach, aby zapewnić pełną ochronę przed kradzieżą tożsamości, korzystanie z takich usług przynosi korzyści. Ponieważ założenie konta kosztuje tylko kilka minut, prawdopodobnie powinieneś to zrobić.

* Monitoruj swoje raporty kredytowe. Jeśli zobaczysz nowe konta, których nie otworzyłeś, natychmiast skontaktuj się z zainteresowaną stroną. Pamiętaj, że jeśli chodzi o oszustwo, im wcześniej zgłosisz problem, tym mniejsze pogorszenie może Cię dotknąć. Skonfiguruj alerty tekstowe. Jeśli wystawca karty oferuje możliwość ustawiania alertów tekstowych, użyj tej funkcji. Dzięki temu otrzymasz powiadomienie, gdy zostaną naliczone opłaty i będziesz mógł działać szybko, jeśli coś będzie nie tak.

* Sprawdź swoje miesięczne wyciągi. Upewnij się, że nadal otrzymujesz wyciągi ze swojego konta tak jak wcześniej i że tak jest nie zostanie źle skierowany do kogoś innego. Przejdź na wyciągi elektroniczne. Jeśli to możliwe, skonfiguruj swoje konto tak, aby otrzymywać miesięczne wyciągi elektroniczne, a nie wyciągi fizyczne, i upewnij się, że otrzymasz wiadomość e-mail i / lub wiadomość tekstową, gdy każdy wyciąg jest wystawiany. Oczywiście należy zadbać o odpowiednią ochronę konta e-mail oraz smartfona, na które wysyłane są takie wiadomości.

Dokumenty wydane przez rząd

Jeśli ktoś włamał się do Twojego paszportu, prawa jazdy lub innego dokumentu tożsamości wydanego przez rząd, należy skontaktować się z agencją, która wydała odpowiedni dokument, i zapytać, jak należy postępować. Dokumentuj wszystko, co ci powiedziano, łącznie ze szczegółami, kto ci co

powiedział. Należy również sprawdzić online w witrynie agencji, czy oferuje ona instrukcje dotyczące takich scenariuszy. W niektórych przypadkach agencje zalecą wymianę dokumentu, co może wymagać fizycznej wizyty w biurze agencji. W innych przypadkach agencja doradzi, aby nic nie robić, ale otaguje Twoje konto, tak aby jeśli dokument był używany do identyfikacji w innych agencjach rządowych, osoby sprawdzające identyfikator wiedziały, że są wyjątkowo czujne (co samo w sobie może być powód do wymiany dokumentu, aby nie napotkać żadnych dodatkowych problemów podczas używania go jako identyfikatora).

Dokumenty wydane przez szkołę lub pracodawcę

Jeśli dane Twojej szkoły lub pracodawcy zostaną naruszone, natychmiast powiadom o tym wystawcę. Informacje te mogą nie tylko zostać wykorzystane do inżynierii społecznej w Twojej szkole lub pracodawcy, ale mogą być potencjalnie wykorzystane do uzyskania poufnych informacji o Tobie od jednego z nich.

Konta w mediach społecznościowych

Jeśli którekolwiek z Twoich kont w mediach społecznościowych zostanie naruszone, natychmiast skontaktuj się z odpowiednim dostawcą mediów społecznościowych. Wszystkie główne platformy mają mechanizmy reagowania na skradzione konta, ponieważ wszystkie główne platformy wielokrotnie miały do czynienia ze skradzionymi kontami. Pamiętaj, że możesz zostać poproszony o dostarczenie dokumentu tożsamości w celu potwierdzenia swojej tożsamości w ramach procesu odzyskiwania konta.