Budowanie i wdrażanie skutecznej polityki bezpieczeństwa informacji

01. Przegląd

Celem tego artykułu jest nakreślenie strategii i zarządzanie procesami przy wprowadzeniem udanej polityki bezpieczeństwa. Dodatkowo, przedstawię zalecenia dotyczące stworzenia Programu Świadomości Bezpieczeństwa, w którym głównym celem będzie zapewnienie lepszego zrozumienia problemów określonych w polityce bezpieczeństwa. Będziemy również koncentrować się na znacznym skróceniu okresu integracji polityki bezpieczeństwa, poprzez odpowiednie wyjaśnienie wszystkich kwestii wskazanych w oficjalnym dokumencie dotyczącym polityki bezpieczeństwa.

02. Zakres

Niniejszy dokument nie ma w założeniu stanowić kompletnego odniesienia do procesu budowania polityki bezpieczeństwa lub opracowania kursu uświadamiającego w zakresie bezpieczeństwa. Zamiast tego został stworzony z myślą o dostarczeniu czytelnikowi rzetelnego źródła porad, różnych zaleceń i przydatnych wskazówek zebranych podczas budowania i rozwijania polityk bezpieczeństwa, a także prowadzenia kursów uświadamiających. W tym dokumencie znajdziesz także przykładowy biuletyn o bezpieczeństwie, najlepsze praktyki dotyczące różnych zagrożeń bezpieczeństwa informacji, a także szczegółowo omówiono niektóre z najczęstszych problemów związanych z bezpieczeństwem, z jakimi zmagają się firmy każdego dnia (koncentrując się w szczególności na problemach bezpieczeństwa zagrażających w jakiś sposób ciągłości i właściwa funkcjonalność instytucji).

03. Wprowadzenie

Bezpieczeństwo informacji zaczęło odgrywać niezwykle istotną rolę w dzisiejszym szybko zmieniającym się, ale niezmiennie technicznie wrażliwym środowisku biznesowym. W związku z tym bezpieczna komunikacja jest potrzebna, aby zarówno firmy, jak i klienci mogli czerpać korzyści z postępów, jakie daje nam Internet. Znaczenie tego faktu musi być wyraźnie podkreślone, aby wdrożono odpowiednie środki, nie tylko poprawiając codzienne procedury i transakcje biznesowe firmy, ale również zapewniając wdrażanie bardzo potrzebnych środków bezpieczeństwa z akceptowalnym poziomem kompetencji w zakresie bezpieczeństwa. To smutne, że w dzisiejszych czasach nieustannie wzrasta możliwość narażenia danych firmy na szkodliwego napastnika, ze względu na dużą liczbę pracowników "analfabetów bezpieczeństwa", którzy mają również dostęp do poufnych, a czasem nawet tajnych informacji biznesowych. Wystarczy wyobrazić sobie bezpieczeństwo osób odpowiedzialnych za poufne dane firmy, niezabezpieczone przeglądanie Internetu w sieci firmy, odbieranie podejrzanych wiadomości e-mail zawierających różne destrukcyjne załączniki i nie zapominajmy o znaczących zagrożeniach wynikających z ciągłego korzystania z komunikatorów internetowych (IM) lub aplikacji do czatu.

04. Dlaczego polityka bezpieczeństwa

Ponieważ budowanie dobrej polityki bezpieczeństwa stanowi podstawę pomyślnej realizacji projektów związanych z bezpieczeństwem w przyszłości, jest to bez wątpienia pierwszy środek, który należy podjąć, aby zmniejszyć ryzyko niedopuszczalnego wykorzystania dowolnego z zasobów informacyjnych firmy. Pierwszym krokiem w kierunku poprawy bezpieczeństwa firmy jest wprowadzenie precyzyjnej, ale możliwej do wyegzekwowania polityki bezpieczeństwa, informowanie pracowników o różnych aspektach ich odpowiedzialności, ogólne korzystanie z zasobów firmy i wyjaśnianie, jak wrażliwe informacje muszą być przetwarzane. Polityka będzie również szczegółowo opisywać znaczenie dopuszczalnego użycia, a także wymienia zabronione działania. Opracowanie (i właściwe wdrożenie)

polityki bezpieczeństwa jest bardzo korzystne, ponieważ nie tylko zamieni wszystkich pracowników w uczestników wysiłków firmy mających na celu zabezpieczenie komunikacji, ale także pomoże zmniejszyć ryzyko potencjalnego naruszenia bezpieczeństwa przez człowieka. Są to zwykle problemy, takie jak ujawnianie informacji nieznanym (lub nieautoryzowanym źródłom), niestabilne lub niewłaściwe korzystanie z Internetu i wiele innych niebezpiecznych działań. Ponadto proces budowania polityki bezpieczeństwa pomoże również zdefiniować kluczowe zasoby firmy, sposoby, w jakie należy je chronić, a także będzie służyć jako dokument scentralizowany, jeśli chodzi o ochronę zasobów związanych z bezpieczeństwem informacji.

05. Co to jest polityka bezpieczeństwa

Polityka bezpieczeństwa to w zasadzie plan, określający, jakie są kluczowe aktywa firmy oraz w jaki sposób muszą (i mogą) być chronione. Jego głównym celem jest dostarczenie personelowi krótkiego przeglądu "dopuszczalnego wykorzystania" dowolnego z aktywów informacyjnych, a także wyjaśnienie, co jest dozwolone, a co nie, a tym samym zaangażowanie ich w zabezpieczanie krytycznych systemów firmy. Dokument działa jak "źródło informacji" dla wszystkich, którzy w jakikolwiek sposób wykorzystują systemy i zasoby zdefiniowane jako potencjalne cele. Dobrze rozwinięta polityka bezpieczeństwa powinna uwzględniać niektóre z następujących elementów:

- Jak wrażliwe informacje muszą być traktowane

- Jak prawidłowo zarządzać swoim ID(-ami) i hasłem(-ami), a także innymi danymi księgowymi

- Jak zareagować na potencjalny incydent bezpieczeństwa, próbę włamania itp.

- Jak bezpiecznie korzystać ze stacji roboczych i połączeń internetowych

- Jak prawidłowo korzystać z korporacyjnego systemu poczty e-mail

Zasadniczo, główne powody, dla których stworzono politykę bezpieczeństwa, to ustanowienie fundacji bezpieczeństwa informacji firmy, wyjaśnienie pracownikom, w jaki sposób są odpowiedzialni za ochronę zasobów informacyjnych, oraz podkreślenie znaczenia zabezpieczenia komunikacji podczas prowadzenia działalności online.

06. Pierwsze kroki

Celem tej sekcji jest przedstawienie możliwych strategii i zaleceń dotyczących procesu tworzenia polityki bezpieczeństwa oraz przedstawienie podstawowego planu podejścia przy tworzeniu ram polityki. Procedura rozpoczęcia tworzenia polityki bezpieczeństwa wymaga pełnej eksploracji sieci firmowej, a także wszystkich innych zasobów krytycznych, aby można było skutecznie wdrożyć odpowiednie środki. Wszystko zaczyna się od zidentyfikowania krytycznych zasobów informacyjnych firmy, tematu, który jest szczegółowo omówiony w następnej części artykułu.

07. Analiza ryzyka (identyfikacja aktywów)

Podobnie jak w każdej innej wrażliwej procedurze, analiza ryzyka i zarządzanie ryzykiem odgrywają istotną rolę w prawidłowym funkcjonowaniu procesu. Analiza ryzyka to proces identyfikacji najważniejszych zasobów informacyjnych firmy oraz jej wykorzystania i funkcjonalności - ważnego (kluczowego) procesu, który należy potraktować bardzo poważnie. Zasadniczo jest to właśnie proces definiujący dokładnie, CO CHCESZ chronić, KOGO próbujesz chronić i, co najważniejsze, JAK zamierzasz go chronić. Aby móc przeprowadzić skuteczną analizę ryzyka, trzeba dobrze zapoznać się ze sposobami działania firmy; w stosownych przypadkach, metody pracy i określone procedury biznesowe, które zasoby informacyjne są ważniejsze od innych (ustalanie priorytetów) i identyfikowanie urządzeń /

procedur, które mogą prowadzić do potencjalnego problemu związanego z bezpieczeństwem. Wymień wszystko, co jest niezbędne dla prawidłowej funkcjonalności procesów biznesowych,podobnie jak kluczowe aplikacje i systemy, serwery aplikacji, serwery WWW, serwery baz danych, różne biznesplany, projekty w fazie rozwoju itp.

Podstawowym podejściem byłoby:

- Określ, co próbujesz chronić

- Zobacz, kogo próbujesz chronić

- Określ potencjalne ryzyko dla któregokolwiek z Twoich zasobów informacyjnych

- Rozważ monitorowanie tego procesu w sposób ciągły, aby być na bieżąco z najnowszymi słabościami w zakresie bezpieczeństwa

Możliwą listą kategorii do obejrzenia jest:

- Sprzęt: Wszystkie serwery, stacje robocze, komputery osobiste, laptopy, nośniki wymienne (dyski CD, dyskietki, taśmy itp.), Linie komunikacyjne itp.

- Oprogramowanie: Zidentyfikuj ryzyko potencjalnego problemu związanego z bezpieczeństwem z powodu przestarzałego oprogramowania, nieczęstych poprawek i aktualizacji nowych wersji itp. Weź również pod uwagę potencjalne problemy z instalowaniem przez pracowników różnych aplikacji do udostępniania plików (Kazaa, Sharereactor, E-Donkey itp. .), Oprogramowanie komunikacyjne (IM), rozrywkowe lub darmowe oprogramowanie pochodzące z nieznanych i niewiarygodnych źródeł.

- Personel: ci, którzy mają dostęp do poufnych informacji, danych wrażliwych, tych, którzy "posiadają", administrują lub w jakikolwiek sposób modyfikują istniejące bazy danych.

08. Zarządzanie ryzykiem (identyfikacja zagrożeń)

W oparciu o badania przeprowadzone na zasobach informacyjnych firmy, powinieneś być teraz w stanie właściwie zarządzać wszystkimi zagrożeniami stwarzanymi przez każdy z Twoich zasobów. Celem tej części jest poprowadzenie Cię przez proces tworzenia listy opisującej różne potencjalne zagrożenia, co również powinno znaleźć się w formalnej polityce bezpieczeństwa. Każdy z poniższych elementów zostanie dokładniej omówiony w dalszej części programu Security Awareness, co zapewni pracownikom lepsze zrozumienie każdego z tematów omówionych poniżej.

- Fizyczne / Desktop Security

Dostęp do systemu: najlepsze praktyki tworzenia haseł, starzenia się haseł, minimalnej długości hasła, znaków, które należy uwzględnić przy wyborze haseł, utrzymywania haseł, wskazówek dotyczących zabezpieczenia (dowolnych) danych księgowych; zagrożenia związane z każdą z tych kwestii należy wyjaśnić w programie podnoszenia świadomości bezpieczeństwa;

Ochrona przed wirusami: najlepsze praktyki ochrony przed złośliwym kodem, jak często system powinien być skanowany, jak często, jeśli nie automatycznie, powinna być przeprowadzana aktualizacja na żywo bazy danych oprogramowania, wskazówki dotyczące ochrony przed (dowolnym) złośliwym kodem (wirusy / trojany / robaki));

Instalacja oprogramowania: czy oprogramowanie freeware jest zabronione, o ile jest dozwolone, w jakich warunkach, w jaki sposób tolerowane jest oprogramowanie, dozwolone są rozrywki lub całkowicie zakazane, a także instalacja jakiegokolwiek innego programu pochodzącego z nieznanych i niewiarygodnych źródeł;

Nośniki wymienne (dyskietki, dyskietki): Należy określić środki "dopuszczalnego użytkowania" (być może za pomocą AUP - zasady dopuszczalnego użytkowania), zagrożenia związane z potencjalnym złośliwym kodem wchodzącym do sieci firmowej lub dowolnego innego krytycznego systemu należy wyjaśnić jako dobrze;

Szyfrowanie: wyjaśnij kiedy, jak i kto musi szyfrować dowolne dane firmy;

Kopie zapasowe systemu: zaleta posiadania kopii zapasowych wymaga wyjaśnienia; kto jest odpowiedzialny i jak często powinny być tworzone kopie zapasowe danych;

Utrzymanie: ryzyko związane z potencjalnym naruszeniem bezpieczeństwa fizycznego należy krótko wyjaśnić;

Postępowanie w przypadku incydentów: zdefiniuj, co jest podejrzanym wydarzeniem, komu należy je zgłosić i jakie dalsze kroki należy podjąć;

- Zagrożenia internetowe

Przeglądanie stron internetowych: określ, co stanowi ograniczoną, zabronioną i potencjalnie złośliwą witrynę internetową, zapewnij członkom personelu krótkie i dobrze podsumowane wskazówki dotyczące bezpieczniejszego przeglądania, dodatkowo informuj ich, że ich użycie w Internecie jest ściśle monitorowane w celu ochrony wewnętrznych systemów firmy;

Korzystanie z poczty e-mail: zdefiniuj kryteria "akceptowalnego użycia" systemu poczty e-mail, co jest dozwolone, a co nie, zasady firmy dotyczące korzystania z systemu pocztowego dla wiadomości osobistych itp. Krótko wyjaśnij potencjalne zagrożenia związane z (nadużywanie) systemu pocztowego i potencjalnych problemów w zakresie rozprzestrzeniania szkodliwego kodu;

Oprogramowanie do przesyłania wiadomości błyskawicznych (ICQ, AIM, MSN itp.): Czy jest dozwolone lub całkowicie zabronione, podaj krótkie przykłady tego, w jaki sposób atakujący może używać tych programów do penetracji i kradzieży / uszkodzenia / modyfikacji danych firmy;

Pobieranie / Załączniki: pobieranie jest dozwolone lub nie, przydatne wskazówki dotyczące bezpiecznego pobierania, objaśnienia zaufanych i niewiarygodnych źródeł, najlepsze praktyki dla załączników do wiadomości e-mail, o ile są dozwolone, omówienie potencjalnych zagrożeń i niebezpieczeństw, wykorzystanie skanerów antywirusowych itp.

Elementy te zostaną później szczegółowo omówione w programie dotyczącym świadomości bezpieczeństwa. Pracownicy muszą zrozumieć, dlaczego niektóre czynności są zabronione, jaki wpływ na firmę mają niektóre zagrożenia, jakie działania należy podjąć w przypadku podejrzenia lub wykrycia potencjalnego problemu związanego z bezpieczeństwem. Angażując pracowników w program świadomości bezpieczeństwa, pracownicy nie tylko poszerzą swoją wiedzę na temat bezpieczeństwa informacji, ale także dowiedzą się, jak zachowywać się w sposób bezpieczny podczas korzystania z zasobów informacyjnych firmy.

09. Naruszenie zasad bezpieczeństwa

Aby zdać sobie sprawę ze znaczenia polityki bezpieczeństwa, pracownicy muszą być świadomi i w pełni zrozumieć konsekwencje naruszenia zasad, eksponując krytyczne systemy dla szkodliwego napastnika lub powodując niezamierzone szkody innym firmom na całym świecie. Naruszenia powinny być odpowiednio traktowane; ci, którzy w taki czy inny sposób naruszają politykę bezpieczeństwa, powinni zostać poinformowani, że mogą zostać narażeni na "okres próbny", który obejmuje również ograniczone wykorzystanie niektórych zasobów informacyjnych firmy, dopóki nie wykażą, że są w

stanie działać w sposób bezpieczny podczas korzystania z systemów korporacyjnych. Powinni także pamiętać, że w niektórych (ciężkich) przypadkach mogą oni również zostać zwolnieni, a nawet ścigani. Podczas gdy dla niektórych może się to wydawać przesadą, należy podjąć odpowiednie działania w każdym przypadku naruszenia, zgodnie z warunkami AUP i polityki, z naciskiem na powtarzanie zasad bezpieczeństwa, a nie kar. W przeciwnym razie najprawdopodobniej dojdzie do pomyślnej penetracji z powodu błędu ludzkiego lub niezrozumienia polityki.

10. Rewizja polityki bezpieczeństwa

Celem tej sekcji jest przeprowadzenie przez ciebie procesu przeglądu Twojej polityki bezpieczeństwa, a także zapewnienie jej skuteczności poprzez uważny przegląd kilku krytycznych czynników, które pozwolą jej osiągnąć trwały sukces. Załóżmy, że już stworzyłeś (lub poprawiłeś) politykę bezpieczeństwa i wygląda ona idealnie dla Ciebie; Ae jak wygląda to dla pracowników? Czy rozumieją każdy z wymienionych terminów, urządzeń lub aplikacji? Jak jasna i precyzyjna jest Twoja polityka; jest to może trochę zbyt szczegółowe lub precyzyjne, że ludzie tracą z pola widzenia to, co próbuje przekazać. Czy jest wręcz przeciwnie, całkowicie pomijając punkt i / lub nie obejmując żadnego z ważnych problemów? Oto niektóre z najważniejszych czynników, które zostaną omówione poniżej. Aby zmniejszyć prawdopodobieństwo nieporozumień, polityka bezpieczeństwa musi w pełni określać obowiązki każdego z pracowników. Powinien jasno określać, co należy chronić, w jaki sposób personel powinien go chronić, a przede wszystkim dlaczego należy go chronić; w ten sposób będą mogli zrozumieć znaczenie i odróżnić krytyczne i mniej krytyczne zasoby informacyjne. Polityka musi być jasna, zwięzła i mieć około dwóch stron. Nie zamieniaj swoich zasad bezpieczeństwa w kompletny kurs na temat bezpieczeństwa; każdy z zawartych w nim elementów powinien być omawiany w Programie Bezpieczeństwa, a nie w Polityce. Zdefiniuj cel polityki bezpieczeństwa od samego początku; dotyczy to aktywów informacyjnych całej firmy lub jest tworzony w celu objęcia konkretnego działu lub działu. Dobrym pomysłem jest zapewnienie użytkownikom lepszego zrozumienia, jak ważne jest bezpieczeństwo informacji dla firmy, wskazując, dlaczego nie ma czegoś takiego jak 100% bezpieczeństwa, ale ryzyko może być znacznie zmniejszone, jeśli wszyscy zdadzą sobie sprawę, że "bezpieczeństwo to odpowiedzialność wszystkich ". Każdy z zasobów musi być precyzyjnie opisany, aby obejmował między innymi takie elementy, jak sprzęt, oprogramowanie, personel, akceptowalne użytkowanie Internetu itp. Jeśli Twoja firma stworzyła już politykę bezpieczeństwa, nie marnuj cennego czasu i zasobów na budowanie nową; po prostu odbuduj i zaktualizuj bieżącą, oszczędzając w ten sposób dużo czasu na badania. Często musisz monitorować i aktualizować swoją politykę bezpieczeństwa, ponieważ nowe zagrożenia i technologie pojawiają się niemal każdego dnia. Staraj się zawsze być na bieżąco z najnowszymi problemami bezpieczeństwa (i związanymi z nimi środkami), aby zasoby informacyjne Twojej firmy były chronione w rozsądnym stopniu. Twoje zasady muszą jasno określać, w jaki sposób można skontaktować się z Biurem Bezpieczeństwa Informacji (ISO) (jeśli istnieje, w przeciwnym razie, odpowiednia osoba kontaktowa); pracownicy muszą wiedzieć, z kim powinni się skontaktować, gdy mają pytania, wątpliwości lub wykryli podejrzane działania. Powinieneś przynajmniej dysponować telefonem (komórkowym) i adresem e-mail dla tego punktu kontaktowego.

11. Wdrażanie polityki

Po opracowaniu, aktualizacji, aktualizacji i uzgodnieniu polityki bezpieczeństwa następuje proces wdrażania nastąpi. Zwykle jest to trudniejsze niż stworzenie samej polityki, ponieważ na tym etapie trzeba również szkolić i kształcić pracowników, aby zachowywali się w "bezpieczny" sposób, przestrzegając każdego z kluczowych elementów wskazanych w formalnej polityce bezpieczeństwa. Ostateczna wersja zasad bezpieczeństwa musi zostać udostępniona wszystkim pracownikom mającym dostęp do dowolnych zasobów informacyjnych. Zasady muszą być łatwo dostępne w dowolnym momencie, z kopią umieszczoną w wewnętrznej sieci i intranecie, jeśli dotyczy. Właściwa

implementacja wymaga nie tylko edukowania personelu o każdym z podstawowych elementów oznaczonych jako krytyczne w formalnej polityce bezpieczeństwa, ale także zmiany ich roli w wysiłkach na rzecz ochrony krytycznych danych firmy. Następna sekcja ma na celu poprowadzenie cię przez proces tworzenia podstawowego programu świadomości bezpieczeństwa, wraz z różnymi nowatorskimi i interesującymi sposobami edukowania twojego personelu, korzystając z przyjaznych dla użytkownika i nieformalnych linii komunikacji między członkami Biura Bezpieczeństwa Informacji (ISO) i Twoi pracownicy.

12. Co to jest program świadomości bezpieczeństwa

Program świadomości bezpieczeństwa można zdefiniować jako jeden z kluczowych czynników skutecznej realizacji polityki bezpieczeństwa obowiązującej w całej firmie. Głównym celem jest określenie konkretnej roli każdego z pracowników w celu zabezpieczenia krytycznych zasobów firmy, a także szczegółowego omówienia każdego z kluczowych elementów wskazanych w polityce bezpieczeństwa. Program ma na celu zwiększenie zainteresowania bezpieczeństwem informacji w łatwy do zrozumienia, ale skuteczny sposób. Program świadomości bezpieczeństwa jest często podzielony na dwie części, z których jedną jest sekcja "świadomość", a druga "szkolenie". Celem świadomości jest zapewnienie personelowi lepszego zrozumienia zagrożeń bezpieczeństwa i znaczenia bezpieczeństwa dla codziennych procedur biznesowych firmy. Część szkoleniowa ma na celu szczegółowe omówienie wielu potencjalnych problemów związanych z bezpieczeństwem, a także wprowadzenie zestawu łatwych do zrozumienia (i przestrzegania) zasad w celu zmniejszenia ryzyka możliwych problemów.

13. Proces rozwoju

W tej sekcji znajdziesz różne strategie budowania solidnego programu świadomości bezpieczeństwa. Omówimy różne metody, ich zalety i wady, a także damy ci lepsze zrozumienie podstawowych kroków do budowania Programu. Na początku musisz odpowiedzieć sobie na następujące pytania:

- Jaki program bezpieczeństwa ma to osiągnąć i jak zamierzasz zwrócić na to uwagę?

- Kim są twoi odbiorcy, jak są "wykształceni"; czy konieczne będzie podzielenie programu na dwie części, jedną dla tych, którzy mają większą wiedzę na temat komputerów, i jedną dla tych, którzy w ogóle nie mają wiedzy na temat komputerów?

- W jaki sposób osiągniesz i zmotywujesz swoich odbiorców? Co ważniejsze, w jaki sposób zachęcisz odbiorców do poprawy zasobów informacyjnych firmy?

- Czy program będzie polegać na formalnym lub nieformalnym sposobie komunikacji między tobą a członkami personelu? W jaki sposób zamierzasz ją przeprowadzić i przedstawić?

Cel programu

Przede wszystkim musisz wyjaśnić pracownikom, co program będzie próbował osiągnąć, jak będzie dążyć do usprawnienia działania firmy i jak istotna jest ochrona zasobów informacyjnych. Będziesz musiał wyjaśnić, dlaczego "bezpieczeństwo należy do wszystkich" i upewnić się, że wszyscy to rozumieją; wyjaśnij, że nawet jeśli firma ma najnowsze udoskonalenia technologiczne, takie jak zapory ogniowe, systemy wykrywania włamań itd., niewykształcony członek personelu może łatwo zagrozić wrażliwym informacjom i sprawić, że wszelkie środki bezpieczeństwa technicznego będą całkowicie bezużyteczne. Innym częstym nieporozumieniem, z którym na pewno spotkasz się podczas prowadzenia Programu, jest to, że większość ludzi często myśli, że nie jest ich obowiązkiem pomoc w poprawie bezpieczeństwa swojej firmy. Ogólnie rzecz biorąc, ludzie mają (złą) opinię, że tylko dział IT

lub Biuro Bezpieczeństwa Informacji (ISO) może i musi zajmować się takimi kwestiami, i to jest to, gdzie ogólnie rzecz biorąc zatrzymują się.

Zwracając się do publiczności

Jednym z głównych problemów, na które na pewno się natkniesz, jest różnica w poziomie umiejętności obsługi komputera (odbiorców), co czasami zmusza do zwrócenia dodatkowej uwagi na tych, którzy nie są aż tak zainteresowani komputerami. Z drugiej strony można również wybrać rozróżnienie między tymi, którzy potrzebują edukacji bezpieczeństwa, a tymi, którzy tego nie robią; chodzi o oddzielenie personelu mającego dostęp do zasobów informacyjnych firmy od tych, którzy tego nie robią (i nie mogą w jakikolwiek sposób narażać wrażliwych danych), ponieważ zdecydowanie zaoszczędzi to wiele czasu i zasobów. Byłoby to dobre podejście do organizowania nieformalnych spotkań z pracownikami, aby rozmawiać na poziomie osobistym, a także przeprowadzać szereg ankiet w celu zmierzenia ich poziomu umiejętności; w ten sposób będziesz wiedział, na co zwrócić uwagę.

Mierzenie poziomu świadomości bezpieczeństwa poprzez ankiety

Ankiety dotyczące bezpieczeństwa są opracowywane z myślą o mierzeniu aktualnego poziomu świadomości pracowników, ale zazwyczaj wskazują także na typowe błędy i nieporozumienia pracowników, co zdecydowanie pomoże ci poprawić jakość programu, nawet zanim się zacznie. Zaleca się archiwizowanie ankiet w celu oceny skuteczności Programu w pewnym okresie. Możesz również wskazać pracownikom, że ankieta jest całkowicie anonimowa, że nie ma potrzeby oszukiwać, ponieważ głównym celem jest jedynie zmierzenie ogólnego poziomu świadomości bezpieczeństwa w firmie, a przede wszystkim, że jest to tylko ankieta i nie egzamin. Mogli odpowiedzieć na główne pytanie bez konieczności odpowiedzi w sekcji "Dlaczego tak sądzą", jeśli nie wiedzą, co tu podać jako odpowiedź.

Niektóre przykładowe pytania z ankiety bezpieczeństwa mogą być:

1. Które z poniższych haseł jest najbezpieczniejsze i dlaczego tak uważasz?

- abc123456

- Herkules

- HRE42pazoL

- $ safe456TY

Dlaczego tak myślisz?

2. Jakie jest najniebezpieczniejsze rozszerzenie załączników i dlaczego tak uważasz?

- * .exe

- * .com

- *.bat

- * .vbs

- wszystkie powyższe

Dlaczego tak myślisz?

3. W twojej polityce bezpieczeństwa jest napisane, że Biuro Bezpieczeństwa Informacji (ISO) nigdy nie wysłałoby ci aktualizacji aplikacji, ale właśnie otrzymałeś jedną, co byś zrobił dalej?

- ponieważ pochodzi z security@company.com, który jest naszym adresem e-mail ISO, uruchomię go i będę miał najnowszą wersję oprogramowania.

- jak stwierdzono w polityce bezpieczeństwa, przed uruchomieniem muszę zeskanować wszystkie załączniki, a następnie skanować i uruchamiać po tym.

- Natychmiast skontaktowałbym się z biurem ISO, aby poprosić o dalsze informacje.

4. Twój przyjaciel dał ci wczoraj wieczorem multimedialną płytę CD, którą zamierzasz sprawdzić naswojej stacji roboczej w pracy; jak zamierzasz to zrobić?

- jest moim przyjacielem i nigdy nie dałby mi żadnych niszczycielskich plików, takich jak wirusy itp. ufam mu / jej, dlatego od razu to sprawdzę.

- chociaż jest moim przyjacielem, w polityce bezpieczeństwa stwierdza się, że nośniki wymienne są dozwolone, ale ich użycie powinno być ograniczone do minimum; Będę się do tego przyzwyczajał i zeskanuję zawartość CD i zobaczę, co jest w środku, zanim to zrobię.

- Po prostu sprawdziłbym zawartość płyty z mojego osobistego komputera.

5. Przedstawiciel biura ISO prosi (osobiście) o hasło, ponieważ je zgubił, i potrzebowałby go do wdrożenia dalszych środków bezpieczeństwa na stacji roboczej, co byś zrobił?

- nie mogą uzyskać dostępu do stacji roboczej bez mojego hasła, a jeśli chodzi o poprawę bezpieczeństwa, oddałbym je, ponieważ to one są odpowiedzialne za utrzymanie bezpieczeństwa w organizacji.

- Mam już odpowiednio zabezpieczoną stację roboczą, więc nie dam jej tego.

- Nie podzielę się z nikim moim hasłem, nawet jeśli mój menedżer próbuje zmusić mnie do tego; Utrzymałbym to w tajemnicy, jak to tylko możliwe.

Oto kilka przykładowych pytań dotyczących większości zagrożeń wskazanych w polityce bezpieczeństwa. To Ty decydujesz, ile pytań powinno być w ankiecie, a także aspekty, które powinny one obejmować; ale zaleca się rozważenie regularnego wydawania ankiet, aby stale monitorować poziom i skuteczność programu.

Przyciąganie ich uwagi

Pracownicy mają już wiele rzeczy do przemyślenia, wiele decyzji do podjęcia, obsługi i uruchomienia przez większość codziennych procedur biznesowych; w związku z tym trzeba mieć bardzo dobrą strategię, aby zmotywować ich do działania i chcieć dowiedzieć się, w jaki sposób mogą poprawić bezpieczeństwo firmy. W dzisiejszych czasach wszyscy interesują się historiami o bezpieczeństwie komputerowym w taki czy inny sposób, zwłaszcza o włamaniach (o wysokim profilu), i korzystając z tego, twoim głównym celem będzie pomóc zrozumieć uczestnikom program, który w rzeczywistości stanie się nowym "odźwiernym" krytycznych danych firmy (aktywów informacyjnych). Bez wątpienia otrzymasz pytania typu "Tak, wspaniale jest przyczynić się do bezpieczeństwa firmy, ale co otrzymam w zamian", które określam jako normalne pytania, na które musisz udzielić właściwych odpowiedzi. Twoi przyszli "studenci" muszą być świadomi i rozumieć, jak drogie jest przedsiębiorstwo, aby prowadzić Kursy Bezpieczeństwa i zatrudnić ekspertów ds. Bezpieczeństwa, aby zapewnić klientom "możliwe do osiągnięcia" usługi. Wyjaśnij im szkody, które mogą zostać wyrządzone firmie, firmie (marce), jej wizerunkowi itp., Co nieuchronnie wpłynie na nich w jakiś sposób w zamian. Z drugiej strony zwracają uwagę na osobiste korzyści płynące z całego programu i wartości całej wiedzy, która zostanie im dostarczona. Dobrym przykładem jest wspomnieć, jak wszystkie te informacje znacznie

pomogą im podnieść poziom bezpieczeństwa własnego komputera osobistego w domu. Informacje, które zostaną im przekazane, odnoszą się nie tylko do komputerów osobistych w pracy, ale również dotyczą (w całości) również ich domowego komputera. Inną ważną kwestią, o której warto pamiętać, są różne sposoby, w jakie ludzie uczą się i zapamiętują, lub innymi słowy, zajmują się informacją, którą właśnie otrzymali. Niektórzy uczą się, czytając materiały, podczas gdy inni uczą się więcej, patrząc na diagramy, chociaż udowodniono, że połączenie tych metod ma maksymalny efekt w procesie zrozumienia tematu. Dlatego musisz upewnić się, że twój styl prezentacji jest taki, że przemawia do tłumu ludzi o różnym stopniu wiedzy i zrozumienia. Wszyscy znudzeni są czytaniem długich materiałów, bez względu na to, jakie są interesujące; jeśli nie ma obrazu, diagramu ani niczego, co wnosi pewien rodzaj różnorodności do procesu, ludzie pozostawiają go w tyle. Staraj się "wizualizować" każdy temat, o którym mówisz, dodając mnóstwo zdjęć, schematów, odpowiednich dzieł sztuki i kreskówek. Kreskówki są szczególnie dobre, ponieważ dodają element humoru; ludzie na pewno zapamiętają zabawną sytuację, która przedstawia daleko poważną procedurę. Komiksy najlepiej nadają się do plakatów i są najskuteczniejsze, gdy są umieszczane w całej firmie, a ich głównym celem jest przyjazne medium do rozpowszechniania komunikatów programu bezpieczeństwa (np. "zablokuj maszynę po jej opuszczeniu" lub "nie dziel się ID i hasłem z KAŻDYM "itp.). Humor odgrywa istotną rolę w przyjaznej edukacji członków personelu; rozważ użycie tego, co uważasz za stosowne, ale nie zamieniaj całego programu w wielką komedię, w której wszyscy się śmieją i po prostu żartują z słowa "bezpieczeństwo". Dodanie małej, zabawnej anegdoty do każdego z twoich wykładów: "Mam przyjaciela, który jest tak paranoikiem w kwestii bezpieczeństwa, że pali wszystkie papiery po pracy, ale chodź, nie ustawiaj alarmów przeciwpożarowych, po prostu dokładne podarcie dokumentów oznaczonych jako poufne / tajne "byłoby w porządku.

Wybór podejścia

Istnieje kilka podejść, które możesz zastosować, gdy kształcisz personel, a ta sekcja wskaże tę, którą określam jako najlepszą; połączenie formalnych i nieformalnych sposobów edukacji. Zaletą metody formalnej jest to, że pomoże to pracownikom zdać sobie sprawę z wagi problemu bezpieczeństwa, ponieważ wiedzą, że prezentacje te pochłaniają sporo zasobów, wysiłku i pieniędzy. Z drugiej strony podkreśli fakt, że firma bardzo poważnie podchodzi do kwestii bezpieczeństwa, a zatem podejmuje bardzo poważne środki w celu ochrony swoich zasobów informacyjnych poprzez edukację swoich pracowników; a wszystko, czego wymaga od nich, to trochę czasu, oddania i zrozumienia wagi problemu bezpieczeństwa. Kolejnym bardzo korzystnym punktem podczas przeprowadzania formalnego programu świadomości jest fakt, że twoje przesłanie, samouczek, prezentacja będą rozłożone pomiędzy większość, jeśli nie wszystkich pracowników; dotrzesz do wielu ludzi w ten sposób, co zaoszczędzi ci dużo czasu w porównaniu do metod takich jak sesje jeden-na-jednego, itp. Nieformalny sposób edukacji składa się z przypomnień e-mailowych, dyskusji, plakatów rozpowszechniających komunikaty zorientowane na bezpieczeństwo (które są w większości omawiane na kursie) , wygaszacze ekranu, podkładki pod mysz, kubki, naklejki itp., ponieważ dyrektorzy ds. bezpieczeństwa stale poszukują nowych i innowacyjnych sposobów edukowania pracowników. Zaletą tej metody jest to, że nie popycha ona (ani nie zobowiązuje) ludzi w żaden sposób, np. do udziału w spotkaniu, słuchania wykładów itp. jest bardzo spersonalizowany, przyjazny dla użytkownika i bardzo skuteczny, ponieważ zbliża się do każdego z nich codzienne życie i procedury pracy w firmie (plakaty, podkładki pod mysz itp.). Nieformalne dyskusje są kolejnym bardzo korzystnym sposobem edukacji i pomiaru umiejętności personelu, w którym ludzie zadają pytania, na które odpowiada przedstawiciel ISO; atmosfera jest zwykle znacznie bardziej nieformalna i spokojna. Jest to wysoce zalecany sposób komunikowania się z pracownikami, ponieważ inicjuje dwukierunkową komunikację ,rozmowa, dzięki której można objąć wiele punktów. Podobnie jak w wielu innych aspektach, musisz znaleźć właściwą równowagę między formalnym i nieformalnym sposobem, ponieważ obie te metody mają swoje różne

zalety i wady. Dzięki uważnemu monitorowaniu reakcji personelu na spotkania i przeprowadzane wykłady będziesz w stanie znacząco zmienić i stale podnosić jakość swojego Programu świadomości bezpieczeństwa. Zawsze zapewniaj personelowi stale rozwijający się sposób edukacji, a tym samym zachowaj ich zainteresowanie, chęć poznania i uczenia się oraz zmniejszanie szansy na nudę, uczestnicząc w jakimkolwiek wydarzeniu Programu.

14. Zarządzanie zagrożeniami bezpieczeństwa

Kiedy już określisz najlepszy sposób edukacji, przygotuj swój plan i strategię, aby zmierzyć poziom umiejętności obsługi komputera swoich pracowników, powinieneś zacząć od omówienia każdego z elementów wskazanych w polityce bezpieczeństwa. Głównym celem tej sekcji jest szczegółowe zbadanie każdego z tych elementów i omówienie różnych zagrożeń, dostarczając gotowych "najlepszych praktyk" na różne tematy. Zachęcamy Cię do włączenia części tej sekcji do własnych Kursów Świadomości Bezpieczeństwa, zapewniając w ten sposób swoim pracownikom lepsze zrozumienie zagadnień omówionych poniżej.

Omówienie zagrożeń fizycznych i komputerowych

Zagrożenia, które zostaną omówione w tej sekcji dotyczą sposobu korzystania ze stacji roboczej, dostępu do stref zastrzeżonych w firmie oraz sposobu obchodzenia się z poufnymi informacjami. Omówię wszystkie możliwe zagrożenia, szczegółowo omówię ich znaczenie i przedstawię różne skuteczne sposoby zarządzania nimi.

Dostęp do systemu

Personel musi być w pełni świadomy swojej odpowiedzialności za utrzymanie w tajemnicy swojego identyfikatora użytkownika i hasła, a to wszystko dlatego, że jest to pierwsza linia obrony w każdym systemie: identyfikacja użytkownika. Wyjaśnij użytkownikowi, że jest całkowicie zabronione udostępnianie swojego identyfikatora i hasła KAŻDEMU, przez KAŻDĄ z osób, od przedstawicieli Biura Bezpieczeństwa Informacji (ISO) do członków rodziny. Bez względu na to, jak głupio może to brzmieć dla niektórych, nie wolno im tego robić; nawet jeśli menedżer poprosi ich o podanie hasła, musisz odrzucić prośbę. W ten sposób NIKT nie może w żadnej sytuacji zmusić ich do ujawnienia swojego identyfikatora i hasła. Znam przypadki, w których menedżerowie próbowali wymusić (lub nawet oszukać) swój personel, aby podał swoje hasła z jakiegoś powodu, aby ocenić poziom świadomości w zakresie bezpieczeństwa; aby sprawdzić, czy spełniają one warunki określone w Polityce bezpieczeństwa, tj. nie udostępniają swojego ID i hasła KAŻDEMU. Zawsze przydatne jest zapewnienie personelowi takich "żywych" przykładów tego, jak ich świadomość może być i jest oceniana. Od pracowników wymaga się, aby nie zapisywali żadnych danych księgowych lub informacji dotyczących identyfikatorów / haseł na luźnych papierach lub notatek lepkich (postit), ani nie zostawiali wrażliwych informacji na białych tablicach (na przykład po spotkaniu, tablicach i / lub tablicach typu flipchart). usunięty), ponieważ mogłoby to spowodować potencjalne włamanie z powodu niewłaściwego posługiwania się poufnymi danymi. Bez względu na to, jak bezpieczni pracownicy mogą myśleć o swoim haśle, nie powinni mieć możliwości przechowywania ich na żadnym z tych kawałków papieru; muszą zrobić co w ich mocy, a zamiast tego zapamiętać. Innym częstym błędem, którego nie można przeoczyć, jest przerażający fakt, że większość użytkowników ukrywa te notatki pod klawiaturą lub w jakimś "tajnym" miejscu, jak to nazywają, wokół swojego biurka; inna działalność, która powinna być całkowicie zabroniona z oczywistych powodów. Ktoś może łatwo znaleźć "tajną" kryjówkę i zapoznać się z ważnymi danymi księgowymi. Musisz również kształcić swój personel w taki sposób, w jaki tworzone są silne hasła. (Bezpieczne) sposoby przetwarzania danych księgowych są opisane w dokumencie "Najważniejsze wskazówki dotyczące haseł", który krótko podsumowuje te dwa aspekty. Załączam przykład "Tworzenie najlepszych zasad tworzenia haseł" oraz przykładową sekcję

"Najważniejsze wskazówki dotyczące utrzymywania haseł" poniżej, która zawiera przegląd tego, co należy wziąć pod uwagę podczas pisania takich dokumentów.

Tworzenie najlepszych praktyk dla haseł

- Hasła muszą składać się z małych (małych) liter, wielkich (wielkich) liter, cyfr i co najmniej jednego znaku specjalnego, takiego jak (! @ # $% ^ & * () _ + |);

- Minimalna długość hasła musi wynosić co najmniej 7 znaków;

- Nie używaj tego samego hasła na kilku komputerach i / lub usługach, które zostały ujawnione, naraziłoby to bezpieczeństwo wszystkich pozostałych za jednym razem. Dobre przykłady

- Ona327 (sA

- @ 865DapzI

- 93Zobacz # -aq

Wszystko to są przykłady dobrych haseł, ponieważ są w pełni zgodne z najlepszymi praktykami tworzenia hasła; w ten sposób zawiera mieszaninę małych liter, wielkich liter, a także cyfr i znaków specjalnych. Złe przykłady

- aaa123bbb

- abcdefg

- 76543210

Pierwszy jest okropny, a każdy poprawnie skonfigurowany program do jej łamania pobierze go w ciągu kilku minut, a nawet nie wspominajmy o drugim i trzecim. Użytkownik z ostatnim hasłem (76543210) najwyraźniej myślał, że będzie to łatwe do zapamiętania hasło, a także bezpieczne, ponieważ jest długie (ish); ale czego użytkownik nie wie ani nie zdaje sobie sprawy z tego, że większość programów łamiących natrafi na to w ciągu kilku sekund (ponieważ hasło podąża za określonym wzorem liczbowym). Dobrym pomysłem może być włączenie do programu Awareness Course pewnej demonstracji w pewnym momencie, dając Twojemu personelowi wyjątkową okazję zobaczenia, jak (hasło) działa oprogramowanie do łamania zabezpieczeń.

Wskazówki dotyczące tworzenia silnych haseł

- Użyj pierwszych liter cytatu, utworu itp., Na przykład "Coś we mnie bierze część ..." będzie "Cwmbc"

- dołącz dwa słowa, dołącz numer, a także znak specjalny, na przykład "run4life #";

- dobra strategia, gdy zapamiętywanie haseł może być następujące:

Załóżmy, że Twoje hasło to Naige453 $ lZ; po pierwsze, wymawiaj to kilka razy w swoim umyśle, następnie zadaj sobie pytanie, jakie jest twoje hasło, odpowiadając na to pytanie w następujący sposób: "Moje hasło jest mieszaniną imienia Naigel (mój znajomy z zagranicy), kilku cyfr i znaku dolara moje hasło zaczyna się i kończy dużą literą, przed ostatnią literą nazwy (L) znajduje się znak dolara ($), a przed znakiem dolara są liczby losowe. Jest to bardzo przydatna i pomocna sztuczka dla każdego, kto próbuje zapamiętać lub zapamiętać swoje hasło. Powtarzając (prawie wyjaśniając) sobie, jakie hasło opisujesz, tak jak zasugerowałem powyżej, jestem pewien, że nie będziesz miał żadnych problemów z przypomnieniem wyrafinowanego, ale mocnego hasła

Zarządzenie hasłem. Najlepsze praktyki

Właściwe przechowywanie poufnych danych, takich jak identyfikator użytkownika i hasło, należy do obowiązków każdego pracownika. W tej sekcji krótko omówiono zasady sprawdzania poprawności haseł.

- NIE udostępniaj swojego identyfikatora (-ów) i hasła (-ÓW) nikomu, ani przedstawicielowi ISO, personelowi pomocy technicznej, członkom rodziny ani swojemu kierownikowi (-om). Nikt nie może zmusić Cię do ujawnienia Twojego identyfikatora użytkownika i hasła w żadnych okolicznościach, pamiętaj o tym. Twoim obowiązkiem jest przechowywanie danych w tajemnicy, jak to możliwe;

- NIE przechowuj swojego identyfikatora (-ów) użytkownika i hasła (-ów) na jakichkolwiek luźnych fragmentach papieru, lepkich (post-it) notatkach, białych tablicach, flipchartach itp .;

- NIE ukrywaj swojego identyfikatora (-ów) użytkownika i hasła (-ów) pod klawiaturą, ani w żadnym innym miejscu, które byłoby "tajną" kryjówką. Zrób co możesz i zapamiętaj to;

- Zmień hasło (y) po upływie określonego okresu odnowienia haseł w polityce bezpieczeństwa;

- Przed wprowadzeniem swojego identyfikatora użytkownika i hasła upewnij się, że nikt Cię nie obserwuje, aby uniknąć tak zwanej techniki "barku".

- Przed użyciem swojego identyfikatora użytkownika i hasła na komputerze innej firmy należy się upewnić, że jest on dobrze chroniony oraz wolny od trojanów i kluczy.

Ochrona przed wirusami

Opierając się na opublikowanych artykułach, prognozach ekspertów, a także na osobistych doświadczeniach, mogę z łatwością stwierdzić, że wirusy nadal będą stanowić poważne zagrożenie dla krytycznych danych biznesowych i będą nadal ewoluować, stając się bardziej wyrafinowanymi, niebezpiecznymi i niszczącymi. Kiedy zaczniesz wyjaśniać, czym jest wirus, ogranicz go do faktów, na przykład jak destrukcyjny jest on, jakie mogą spowodować szkody, możliwe straty finansowe związane z epidemią wirusa itp. Nie zawracaj sobie głowy pracownikami informacje takie jak sposoby działania wirusów, sposób ich ukrywania i wiele innych tematów, które nie będą dla nich interesujące. Zamiast tego, zapewnij najbardziej zainteresowanym, niektóre zewnętrzne (internetowe) linki do tematu. Rozważ wyjaśnienie, czym jest wirus / trojan / robak, podstawowe funkcje każdego z nich, jak rozpoznać (działanie) jednego z nich w systemie (ach), potencjalne problemy, które mogą one wywoływać, oraz niszczące skutki dla całego systemu. firma. Dostarczaj im żywych przykładów, krótko omawiaj i odpowiadaj na najprostsze i najczęstsze pytania, takie jak "Czy dane mogą zostać uszkodzone przez wirusy" lub "Co zrobić po zarażeniu wirusem?". Należy jednak wyraźnie wyjaśnić, że pomysł prezentacji ma przede wszystkim zapobiegać infekcji, ponieważ po zainfekowaniu szkodliwym wirusem nie ma tak wiele możliwości, szczególnie jeśli nie są to kopie zapasowe danych, z drugiej strony trzeba dokładnie wyjaśnić, jakie szkody osobowe mogą powstać po infekcji wirusem, uszkodzenia i / lub potencjalną utratę krytycznych danych biznesowych, dokumentów, projektów, planów biznesowych, prezentacji, które już pracowały wraz z wszelkimi innymi danymi osobistymi przechowywanymi na komputerze zostanie zniszczony lub, co bardziej prawdopodobne, zostanie zniszczony. Dzięki poznaniu niszczących skutków wirusów pracownicy będą bardziej świadomi tego tematu i będą bardziej prawdopodobnie zrozumieją wagę tematu i ryzyko zarówno dla ich firmy, jak i domowego komputera. Przejrzyj wiele scenariuszy, w jaki sposób wirusy mogą dostać się do sieci firmowych, w jaki sposób można wprowadzić pracowników w wirowanie, zagrożenia związane z pobieraniem Internetu, problemami z nieaktualnymi sygnaturami wirusów itp. Wyjaśnij także, że skanery antywirusowe (AV) nie są najlepszym, "głupim" rozwiązaniem i sposobem, w jaki polegają na sygnaturach (plikach wzorów). Porozmawiaj o tym, jak przydatne są skanery antywirusowe oraz w jaki sposób skuteczność

stosowanych środków zapobiegawczych w dużej mierze zależy od świadomości i czujności samych użytkowników. Personel musi zrozumieć, że naszym głównym celem jest zapobieganie, a nie działanie po zainfekowaniu; chociaż z pewnością będą infekcje, możemy znacznie zmniejszyć ryzyko infekcji i ograniczyć potencjalne szkody poprzez edukowanie personelu i uświadamianie zagrożeń stwarzanych przez złośliwy kod i oprogramowanie (wirus / trojan / robak). Należy również podkreślić zalety regularnego skanowania systemu, a także potencjalne problemy z niezeskanowaniem systemów; chociaż wiedzą, że skanery AV nie wykryją nowych wirusów, będą wiedziały przynajmniej, że mogą zmniejszyć ryzyko i właściwie zarządzać niebezpieczeństwem. Skanowanie systemów przy użyciu przestarzałych plików sygnatur jest kolejnym typowym problemem, który należy wziąć pod uwagę. Pracownicy powinni aktualizować oprogramowanie antywirusowe / anty trojanowe co najmniej raz w tygodniu, a jeśli oprogramowanie pozwala na scentralizowane automatyczne aktualizacje (większość robi), aktualizacje muszą być regularnie planowane, aby zapewnić wykrywanie przez oprogramowanie najnowszych wirusów / trojanów / robaki (znane laboratorium twojego dostawcy). Różne sposoby zarażenia złośliwym kodem również powinny być prześwietlone; pozwól pracownikom otwarcie zadawać pytania: zobacz, jak reagują na pytania typu "Jak się zaraziłem", a następnie dostarczę im lepszego lub bardziej kompletnego wyjaśnienia na temat najczęstszych, a także konkretnych sposobów infekcji.

Poniżej zamieściłem przykładową sekcję "Najlepsze praktyki dotyczące szkodliwych kodów" dla wygody użytkownika; w żadnym wypadku nie jest to wyczerpująca lista, ale przynajmniej będziesz w stanie zorientować się, co uważa się za niebezpieczną działalność.

Sprawdzone metody złośliwego kodu

- NIE uruchamiaj żadnych plików bez uprzedniego ich skanowania, bez względu na to, czym jest rozszerzenie pliku, tj. (.Exe, .bat, .com, .doc, itp.);

- NIE pobieraj żadnych plików i / lub programów z nieznanych źródeł; w razie wątpliwości należy jak najszybciej skontaktować się z biurem ISO;

- NIE otwieraj załączników, nawet jeśli zostały wysłane przez znajomego lub członka rodziny; najpierw sprawdź, czy wysłał ci plik, ale mimo to skanuj przed otwarciem / uruchomieniem czegokolwiek;

- NIE uruchamiaj żadnych programów znalezionych na dyskietkach / płytach CD na biurku, jeśli nie masz całkowitej pewności, że są one twoje; ktoś mógł umieścić go tam specjalnie, abyś mógł go "znaleźć i sprawdzić";

- Jeśli pobieranie jest dozwolone, ogranicz je do minimum; jeśli potrzebujesz konkretnej aplikacji lub czegoś innego, zawsze skontaktuj się z działem IT lub biurem ISO w celu uzyskania dalszych informacji PRZED pobraniem i zainstalowaniem czegoś;

- Skanuj (pełne skanowanie systemu) co najmniej raz w tygodniu za pomocą domyślnego oprogramowania skanera AV. Przed wykonaniem tej czynności należy zaktualizować sygnatury wirusów, a także rozważyć automatyzację procesu, planując skanowanie całego systemu w celu wygodnego regularnego skanowania w przyszłości;

- Aktualizuj pliki sygnatur tak często, jak to możliwe, aby zapewnić wykrywanie najnowszych złośliwych wzorców oprogramowania;

- Dział IT lub Biuro Bezpieczeństwa Informacji zazwyczaj NIE wysyła do ciebie najnowszych aktualizacji żadnego oprogramowania (chyba że jest to poprzedzone szeroko reklamowaną, dobrze reklamowaną kampanią skierowaną do całej firmy). Jeśli wykryjesz podejrzaną aktywność, nie usuwaj otrzymanej

wiadomości e-mail i skontaktuj się z zespołem ds. obsługi incydentów lub działu pomocy technicznej tak szybko, jak to możliwe;

- jeśli masz jakiekolwiek wątpliwości dotyczące złośliwego oprogramowania (wirusów / trojanów / robaków), natychmiast skontaktuj się z ISO, działem pomocy technicznej lub działem IT. W ten sposób zapobiegniesz potencjalnym niszczącym nieszczęśliwym wypadkom z powodu niewłaściwego i błędnego obchodzenia się z niebezpiecznymi i szkodliwymi incydentami.

Wszystko, co jest zdefiniowane jako zakazane, musi zostać omówione i wyjaśnione; dlaczego jest zabronione lub ograniczone, w jaki sposób może zaszkodzić firmie lub firmie, itp. Rozgryź kilka potencjalnych scenariuszy, pomagając użytkownikom w zrozumieniu tematu w łatwy do zrozumienia sposób, próbując dotknąć podstawy konsekwencji wszystkich tych niebezpieczne działania.

Instalacja oprogramowania

Oprogramowanie typu freeware lub innego typu, uzyskane lub pobrane z nieznanych lub niewiarygodnych źródeł, może łatwo wpłynąć na bezpieczeństwo firmy, ujawnić krytyczne dane biznesowe i / lub uszkodzić newralgiczne dane. Wielu użytkowników zazwyczaj instaluje takie programy (od wygaszaczy ekranu po gry i zabawne kreskówki w programie Flash), jak to mówią, dla różnych osobistych potrzeb i działań; bawić, mieć coś miłego do obejrzenia lub zrelaksować się. Jednocześnie nie zdają sobie sprawy z potencjalnych zagrożeń, na jakie narażają systemy i sieci firm, od złośliwego oprogramowania (wirusy / trojany / robaki) po prawne działania przeciwko firmie w celu zainstalowania (być może) pirackie oprogramowanie na stacji roboczej firmy. Dlatego musisz zapoznać użytkowników z potencjalnymi problemami związanymi z każdym z tych problemów, a także wyjaśnić zasady firmy dotyczące instalowania dowolnego (nieautoryzowanego) oprogramowania na dowolnej stacji roboczej firmy. Pliki pobrane z Internetu, skopiowane z dysku CD lub dyskietki pochodzącej z nieznanego źródła lub wszystko, co nie zostało sprawdzone przez Biuro Bezpieczeństwa Informacji lub nie zostało przeskanowane pod kątem potencjalnie złośliwego kodu (przez korporacyjne systemy AV), może być klasyfikowane jako niewiarygodne, nieznane i niebezpieczne. Bezpłatne aplikacje, ze względu na ich pochodzenie, stanowią poważne źródło zagrożenia i należy się z nimi ostrożnie podchodzić. Pracownicy muszą być świadomi związanego z tym ryzyka i nauczyć się myśleć dwa razy, zanim podejmą działania. Te mogą być stymulowane na wiele sposobów, przedstawiając różne scenariusze dotyczące tego, w jaki sposób oprogramowanie pobrane z Internetu lub skopiowane z jakichkolwiek nośników do usuwania może narazić firmę, jej firmę, prywatność lub wykorzystanie przepustowości firmy na popełnianie nielegalnych działań. Decyzja o tym, czy użytkownicy powinni mieć prawo pobierać i / lub instalować programy innych firm na swoich stacjach roboczych, zależy wyłącznie od Ciebie, oraz wdrożenia odpowiednich zasad (procedur) bezpieczeństwa, które są zgodne z tą decyzją. Konieczne będzie nie tylko wyraźne określenie konsekwencji dla tych, którzy naruszają jakiekolwiek ograniczenia, ale także zapewnienie procedur uzyskiwania i instalowania nowego oprogramowania . Zdecydowanie zaleca się, aby użytkownicy nie mieli możliwości instalowania nowych programów, które mogłyby ujawnić poufne dane firmy, marnować cenną przepustowość lub uszkodzić krytyczne dane. Jeśli użytkownicy potrzebują nowego oprogramowania zainstalowanego do użytku biznesowego, powinni skontaktować się ze swoim kierownikiem, działem IT / IS, działem pomocy technicznej lub ISO (w zależności od procedur określonych w polityce) zamiast samodzielnie podejmować takie działania.

Removable Media (CD, dyskietki, taśmy itp.)

Nośniki wymienne, takie jak dyski CD, dyskietki (dyskietki), a nawet taśmy (taśmy kopii zapasowych / ADR / DAT / DLT) można zdefiniować jako inny możliwy punkt wejścia dla niebezpiecznych i złośliwych plików wchodzących do sieci firmy lub narażających na niebezpieczeństwo jedną stację roboczą. Z

drugiej strony mogą one również służyć do nielegalnego kopiowania poufnych danych, po czym łatwo będzie wyjść z lokalu ze skradzionymi informacjami. Złośliwe oprogramowanie (wirusy / konie trojańskie / robaki) również wykorzystuje do rozprzestrzeniania się nośniki wymienne; niektórzy korzystają z funkcji automatycznego uruchamiania płyty CD (automatycznie uruchamiając plik automatycznego uruchamiania na płycie CD, który może być destrukcyjny), inni nadal używają "klasycznych" metod, takich jak dyskietki, aby zainfekować stację roboczą złośliwym programem. Aby uzyskać najlepsze rezultaty, nośniki wymienne powinny być całkowicie zablokowane (przy użyciu blokad napędu dyskietek lub stacji roboczych bez CD), ale płyty CD mogą być nadal używane na przykład przez wieże CD-ROM. Jeśli potrzebujesz użyć nośnika wymiennego w swoim organizacji, następnie należy ustanowić najlepsze praktyki, omówić możliwe ryzyka i scenariusze zagrożeń, aby zmniejszyć liczbę szkodliwych programów wprowadzanych do sieci we wszystkich punktach, chroniąc w ten sposób firmę przed poważną katastrofą.

Szyfrowanie

Szyfrowanie może być zdefiniowane jako kolejna miara "musisz implementować", która nie tylko zapewni ochronę wrażliwych i krytycznych informacji przed potencjalnym intruzem, ale także ochroni Cię przed wieloma problemami, jeśli w końcu dojdzie do naruszenia bezpieczeństwa. W polityce bezpieczeństwa i procedurach bezpieczeństwa należy jasno zdefiniować systemy, pliki i dokumenty, które powinny być szyfrowane, przez kogo i co najważniejsze, za pomocą jakich algorytmów. Zdecydowanie zaleca się stosowanie sprawdzonych standardowych algorytmów, takich jak DES, IDEA, Blowfish lub RC5.

Kopie zapasowe systemu

Plany odzyskiwania po awarii (DR) mają zasadnicze znaczenie dla ciągłości działalności, a także prawidłowej funkcjonalności bieżących procesów. Wcześniej czy później nieuchronnie zmierzysz się z problemem, w którym system ulega awarii, bez względu na używany system operacyjny, ale można to szybko rozwiązać, jeśli odpowiednie procedury tworzenia kopii zapasowych i plany przywracania po awarii są na miejscu. Będziesz musiał zdefiniować zasoby, które muszą być regularnie archiwizowane, osoby odpowiedzialne, najlepsze praktyki i procedury, a także miejsce przechowywania kopii zapasowych, np. Sejf ognioodporny, sejf, miejsce poza domem itp.

Konserwacja

Odpowiednia konserwacja komputera / stacji roboczej to kolejna istotna kwestia, której nie wolno przeoczyć w trakcie Programu świadomości bezpieczeństwa. Stacje robocze użytkowników stanowią istotne źródło zagrożenia dla bezpieczeństwa firmy, często atakowane przez tzw. "wewnętrznych", szukających niechronionych stacji roboczych. W związku z tym należy również szkolić pracowników w zakresie bezpieczeństwa fizycznego; ponownie można to osiągnąć, przeglądając możliwe scenariusze, zapewniając jednocześnie wskazówki dla lepszej ogólnej ochrony.

Obsługa incydentów

Do tego czasu Twoi pracownicy powinni być w stanie określić potencjalny problem z bezpieczeństwem, podczas gdy powinieneś ustalić zasady postępowania w przypadku wystąpienia incydentu. W swojej polityce musisz jasno określić, co należy zrobić w różnych sytuacjach; Główną ideą powinno tu być minimalizowanie i ograniczanie szkód. Personel powinien zostać poinformowany, kto jest odpowiedzialny za rozwiązywanie problemów i z kim powinni się skontaktować, gdy tylko podejrzewają potencjalny problem z bezpieczeństwem.

Omówienie zagrożeń internetowych

Jednym z największych zagrożeń bezpieczeństwa w firmie jest łączność z Internetem i jej niewłaściwe wykorzystanie przez (niewykształconych) pracowników. Faktem jest, że większość pracowników będzie surfować po witrynach, które są surowo zabronione, a najprawdopodobniej w końcu zostaną pobrane złośliwe pliki i / lub wrogi kod ze stron hakerskich. Każda z tych czynności może wpłynąć na wydajność Twojej firmy, szczególnie jeśli myślisz o procesie odzyskiwania, próbując naprawić błędy popełnione przez pracowników. Dlatego zawsze dobrze jest wyjaśnić szczegółowo możliwe zagrożenia związane z surfowaniem po Internecie; że nie trzeba pobrać cokolwiek, aby zainfekować komputer wirusem, trojanem lub nawet robakiem, ale samo wejście na stronę wystarczy, aby spowodować problem. Określ, co stanowi "zabronione witryny" i wyjaśnij, dlaczego jest to zabronione, w tym problemy, które mogą wystąpić po prostu odwiedzając go.

Przeglądanie sieci

Przeglądanie sieci stanowi zagrożenie dla bezpieczeństwa stacji roboczej, a także dla całej organizacji. Bycie narażonym na niebezpieczeństwa związane z przeglądaniem stron internetowych jest bardzo łatwe, ponieważ wrogie skrypty mogą być pobierane i wykonywane automatycznie; wystarczy na przykład przestarzała wersja przeglądarki internetowej. Personel powinien mieć możliwość odróżnienia witryn sklasyfikowanych jako dozwolone, zakazane lub potencjalnie niebezpieczne i unikać odwiedzania zabronionych. Java i ActiveX powinny być domyślnie wyłączone (nie spowoduje to problemów z dostępem do stron), należy zachować ostrożność przy filmach Flash itp. I jeśli kiedykolwiek pojawi się podpowiedź problemu, należy natychmiast skontaktować się z biurem ISO. W sieci są strony internetowe, które mogą próbować skanować / zalewać sieć, odwiedzając je; Innym wariantem tego (teoretycznego, ale bardzo możliwego) scenariusza jest to, że jeden z pracowników używa jakiejś usługi skanowania, aby sprawdzić bezpieczeństwo swojej stacji roboczej, marnując w ten sposób cenną przepustowość. Coś takiego nieuchronnie przyniesie więcej pracy dla biura ISO, a ich systemy prawdopodobnie zarejestrują użycie tej usługi jako możliwą próbę włamania. Gry hazardowe online i witryny pornograficzne powinny być w pełni zabronione, a korzystanie z Internetu przez pracowników jest monitorowane w celu zapewnienia, że przestrzegają zasad i przepisów określonych w programie Security Awareness.

Korzystanie z poczty e-mail

Zasadniczo systemy poczty e-mail firmy są obszarem wysokiego ryzyka ze względu na ich stałą dostępność do świata zewnętrznego, a ryzyko często jest dwojakie. Wykorzystanie poczty e-mail do prowadzenia działalności gospodarczej, kontakt z klientami i jej integracja w wielu innych procesach biznesowych naraża firmowe adresy pocztowe i systemy (pocztowe) potencjalnym napastnikom. Z drugiej strony jest to również numer jeden, z którego większość szkodliwych programów wchodzi do firmy. Dlatego dobrze znany i sprawdzony program ochrony przed złośliwym kodem jest konieczny we wszystkich bramach pocztowych, ponieważ wykrywa, blokuje i / lub odfiltrowuje większość znanych niebezpiecznych plików i wrogich skryptów próbujących wejść do sieci firmowych. Podobnie jak w przypadku wszystkich aspektów bezpieczeństwa IT, bezpieczeństwo całej firmy można poprawić jedynie poprzez odpowiednie kształcenie personelu. Dlatego zaleca się, aby ustanowić najlepsze praktyki dotyczące korzystania z poczty e-mail, koncentrując się na poniższych punktach.

E-mail Korzystaj ze sprawdzonych metod

- Jeżeli załączniki (e-mail) są dozwolone, załącznik (-i) muszą zostać zeskanowane przed otwarciem, a także potwierdzenie przez nadawcę (tj. Przez telefon), że rzeczywiście załącznik został wysłany. Zmniejszy to również ryzyko uruchomienia programu, który został automatycznie wysłany pocztą elektroniczną (nieznany inicjatorowi) za pośrednictwem jakiejś złośliwej aplikacji, która wykorzystała

konta pocztowe i / lub system pocztowy nadawcy. Jeśli załączniki są zabronione, postępuj zgodnie z zasadami i nie pobieraj / uruchamiaj wszelkich plików otrzymanych jako załączniki;

- Java i ActiveX muszą być wyłączone podczas czytania wiadomości e-mail w celu zarządzania ryzykiem automatycznego uruchamiania złośliwych programów. Podobnie jak w przeglądarce internetowej, niektóre opcje programu można zazwyczaj ustawić i zablokować za pomocą zasad systemowych, które automatycznie ustawiają te warunki dla wszystkich użytkowników podczas logowania;

- Nie używaj firmowych kont e-mail do jakichkolwiek celów rejestracji i nie używaj ich podczas publikowania wiadomości na forach internetowych lub grupach dyskusyjnych. Możesz utworzyć jedno, specjalne (prawdopodobnie aliasowane) konto tylko w tym celu;

- Nie używaj firmowego systemu e-mail do prowadzenia własnego biznesu, nadmiernej korespondencji osobistej, wysyłania dużych załączników, a tym samym marnowania cennej przepustowości;

- Nie odpowiadaj na łańcuszki lub inny rodzaj spamu za pomocą firmowych systemów poczty e-mail; w razie wątpliwości skontaktuj się z biurem ISO;

- Nigdy nie przesyłaj żadnych firmowych danych do zewnętrznych kont e-mail (np. Wyślij dokument roboczy na swoje domowe konto e-mail, aby móc pracować nad nim dalej w domu wieczorem), bez wcześniejszego sprawdzania ze swoim przełożonym i / lub kontaktowaniem się z biurem ISO;

- Właściwe korzystanie z systemu poczty elektronicznej powinno być stale monitorowane, a użytkownicy powinni być świadomi, że mogą zostać pociągnięci do odpowiedzialności za nielegalne działania, takie jak spamowanie, wysyłanie i otrzymywanie nielegalnych wiadomości itp.

Aplikacje do przesyłania wiadomości błyskawicznych (ICQ, AOL, MSN itp.)

Wielu użytkowników zazwyczaj korzysta z tych programów, aby komunikować się ze znajomymi, wysyłać i odbierać załączniki, wiadomości itp., ponieważ te aplikacje często próbują oszukać bramę blokującą zawartość na poziomie serwera, aby umożliwić przekazywanie treści. Jednak nie w pełni zdają sobie sprawę z niebezpieczeństw związanych z tymi programami i potencjalnych szkód, jakie mogą one spowodować. Bez względu na to, z której aplikacji Instant Messaging korzystasz, zawsze możesz zostać zainfekowany lub wykorzystany; przez konkretny błąd aplikacji, o którym nigdy nie słyszałeś, lub wersję buggy, której nigdy nie przejąłeś aktualizacji. Jeśli chodzi o wymianę informacji i plików bez względu na to, gdzie, od kogo i w jaki sposób, należy pamiętać, że istnieją pewne niebezpieczeństwa związane z tym; zdaj sobie sprawę z możliwych niebezpieczeństw twoich działań i twojej naiwności i postępuj zgodnie z nimi.

Pobieranie

Pobieranie jakichkolwiek danych z nieznanych i niewiarygodnych źródeł podczas korzystania z systemów i sieci firmy może mieć druzgocący wpływ na procesy biznesowe; możesz stanąć w obliczu utraty danych, uszkodzenia lub, w niektórych przypadkach, modyfikacji. Należy zatem dążyć do wykształcenia personelu w zakresie procedur pobieranie informacji w bezpieczny sposób; polega to na zapewnieniu pobierania plików tylko wtedy, gdy jest to absolutnie konieczne, skanowaniu pobranych plików za pomocą korporacyjnego rozwiązania Anti-Virus / Anti-Trojan przed jego otwarciem itp. Dla Twojej wygody stworzyliśmy podsumowanie "Najlepsze praktyki korzystania z Internetu" poniżej; Ponownie, nie będąc wyczerpującą listą, ma ona na celu wskazanie podstawowych wskazówek dotyczących bezpiecznego korzystania z Internetu.

Korzystanie z Internetu Najlepsze praktyki

- Java i ActiveX są domyślnie blokowane. Skrypty zawierające Javę i ActiveX stanowią wielkie niebezpieczeństwo ze względu na ich niezabezpieczony charakter, a wynikające z tego problemy mogą mieć druzgocące skutki na twoim komputerze, nie wspominając o firmie. Nie blokuj, nie zatrzymuj ani nie manipuluj przy jakichkolwiek środkach (np. Zasady grupowe), które są stosowane w celu odfiltrowania tych działań, a jeśli masz problemy z zakupem produktu lub odwiedzeniem zaufanej strony internetowej, skontaktuj się z działem IT, działem pomocy lub ISO biuro pomocy;

- Nie odwiedzaj niewłaściwych stron internetowych zawierających kontrowersyjne treści; pornografia, hazard, warez (pirackie oprogramowanie), witryny hakerskie / hakerskie, a także te ogólnie uznane za zabronione przez waszą politykę bezpieczeństwa;

- Jeśli dozwolone jest korzystanie z komunikatorów internetowych, nie przyjmuj żadnych załączników bez względu na typ pliku, rozszerzenie czy źródło.

- Pobieranie oprogramowania, plików lub czegokolwiek innego jest zabronione. Jeśli potrzebujesz aplikacji do codziennej pracy, skontaktuj się z działem IT, działem pomocy technicznej lub biurem ISO. Będziesz najprawdopodobniej musiał złożyć wniosek (oprogramowanie) podpisany przez kierownika, aby ukończyć proces. Jeśli uzyskasz zgodę na pobranie oprogramowania, pamiętaj, aby nigdy go nie uruchamiać przed skanowaniem ich za pomocą korporacyjnego oprogramowania antywirusowego / anty-trojańskiego;

- Cała aktywność internetowa powinna być stale monitorowana, a użytkownicy powinni być świadomi, że mogą zostać pociągnięci do odpowiedzialności za odwiedzanie zabronionych stron internetowych, pobieranie nielegalnych plików i treści, a także ponosić karę za ograniczenie dostępu do Internetu (dopóki nie mogą udowodnić, że są w pełni świadomi ryzyka związanego z ich działaniami).

15. Innowacyjne, ale skuteczne metody edukacyjne

Teraz zrozumieliśmy, że bezpieczeństwo można poprawić tylko poprzez odpowiednie kształcenie personelu. Jednak poziom sukcesu można zawsze poprawić poprzez zmianę metod edukacji; zapewniając, że masz świeży, ciągle rozwijający się i do pewnego stopnia dynamiczny program edukacyjny, przyciągniesz ciągłe zainteresowanie swoimi sesjami edukacyjnymi. Utrzymując ludzi w ciągłym zainteresowaniu i dotarciu do dużej liczby osób, na pewno odbiorcy oczekują niecierpliwie na następne spotkanie. Poniżej opiszę różne metody, które okazały się bardzo udane i jestem pewien, że się zgodzisz po wdrożeniu / ocenie ich skuteczności.

Security Newsletter

Ciekawym i cennym sposobem dotarcia do pracowników i ich edukacją jest niewątpliwie wydawanie Newslettera o bezpieczeństwie za pośrednictwem poczty e-mail. Możesz także dać pracownikowi dodatkową opcję wysyłania biuletynu na swój prywatny adres e-mail, więc nawet jeśli nie będą mieli czasu, aby go przeczytać w pracy, będą mieli taką możliwość później. , z domu. Główną ideą utworzenia biuletynu dotyczącego bezpieczeństwa jest dostarczenie użytkownikom interesującego i wciągającego sposobu zrozumienia punktów określonych w polityce bezpieczeństwa. Aby lepiej zilustrować tę ideę, stworzyliśmy dla Ciebie przykładowy "Newsletter bezpieczeństwa":

Przykładowy biuletyn zabezpieczeń

<Nazwa firmy> Security Newsletter

Numer 1 - MM.DD.RRRR

http://company.com/security/

email: security@company.com

telefon: 123-456-789

987-654-321 Zewn. 000

01.Przyszłe wydarzenia

02. Artykuł o bezpieczeństwie

03.Co to jest ...?

04. Zapytaj nas

05. Zasoby bezpieczeństwa

06.Contacts

1 - Nadchodzące wydarzenia

Ta sekcja zawiera informacje o zbliżających się spotkaniach, dyskusjach, sesjach wykładowych i wszystkim, co dotyczy działań związanych z programem Security Awareness.

2 - Artykuł bezpieczeństwa

Dobrym pomysłem jest dostarczenie swoim pracownikom szczegółowej, dogłębnej informacji na określony temat za pośrednictwem biuletynu, co pomoże im lepiej zrozumieć dany temat. Załóżmy, że na ostatnim spotkaniu dotyczącym świadomości bezpieczeństwa omówiłeś temat "Zagrożenia e-mailowe", więc aby uzyskać maksymalne korzyści ze spotkania, dobrym pomysłem byłoby zamieszczenie artykułu na ten temat tuż po ostatniej sesja świadomości, kiedy wszystko, co mają, jest wciąż świeże w ich pamięci. Nie popełniaj błędu polegającego na umieszczeniu całkowicie nieistotnego artykułu na ostatnim spotkaniu poświęconym bezpieczeństwu, ponieważ spowoduje to dezorientację personelu lub, w najgorszym przypadku, całkowite wyłączenie go z tematu. Staraj się, aby artykuły były krótkie i łatwe do zrozumienia; nie ma potrzeby pisania pełnego eseju na ten temat, chodzi o to, aby zapewnić im dynamiczny sposób edukacji, a także inne nieformalne, ale precyzyjne i dobrze podsumowane podsumowanie tematów z ostatniego spotkania. Artykuły, które możesz rozważyć, obejmują:

- Zabezpieczenie hasłem: Omówienie znaczenia haseł i ich kluczowej roli w ochronie danych firmy, prawidłowego przechowywania identyfikatorów i haseł, tworzenia i utrzymywania haseł, najlepszych praktyk itp .;

- Dopuszczalne korzystanie z Internetu: Omówienie możliwych zagrożeń związanych z łącznością internetową i personelem rzeczy powinien być świadomy (bezpiecznego) przeglądania sieci, prawidłowego korzystania z systemu wiadomości e-mail, co zmniejsza ryzyko rozprzestrzeniania się złośliwego kodu świat, a w tym przypadku, wokół sieci firmowej;

- Dlaczego oni celują w nas? Ciekawy temat, omawiający motywację różnych napastników, który jest zazwyczaj bardzo interesującą lekturą dla wszystkich, zapewniając użytkownikom lepsze zrozumienie znaczenia posiadania odpowiednich środków bezpieczeństwa informacji wdrożonych w firmie;

- Twoja rola w ochronie firmy: możesz myśleć o tylu scenariuszach, ile uznasz za stosowne; Ideą tych artykułów jest wyjaśnienie najważniejszych aspektów bezpieczeństwa informacji w nieformalny, ale

skuteczny sposób i uwzględnienie aspektów społecznych w połączeniu z krótkimi wyjaśnieniami technicznymi, jeśli zajdzie taka potrzeba.

3 - Co to jest ...?

Ta sekcja powinna zostać stworzona z myślą o kształceniu lub informowaniu personelu, aby działał jako glosariusz bezpieczeństwa informacji (IS), gdzie różne warunki bezpieczeństwa są wyjaśnione w nietechnicznym, łatwym do zrozumienia sposobie. Rozważ dodanie maksymalnie trzech terminów w każdym wydaniu, odnoszących się do tematów i artykułów omawianych na ostatnim spotkaniu dotyczącym świadomości bezpieczeństwa ("security awareness") i utrzymuj je bardzo krótkie, ale jednocześnie bardzo informacyjne. Można uwzględnić ogólne tematy bezpieczeństwa, takie jak "Co to jest trojan" lub "Co to jest robak" i "Co to jest zapora", a także wiele innych, które można zdefiniować jako artykuły przydatne i "niezbędne".

4 - Zapytaj nas

Jeśli chodzi o edukację i szkolenie użytkowników za pośrednictwem biuletynu dotyczącego bezpieczeństwa, uważam tę sekcję za najbardziej skuteczną i wartościową; zapewnia bezpośredni i nieformalny sposób komunikacji między Biurem Bezpieczeństwa Informacji (ISO) a pracownikami, którzy z kolei mają możliwość kierowania swoich pytań związanych z bezpieczeństwem do przedstawiciela ISO. Pytania i odpowiadające odpowiedzi powinny następnie zostać uwzględnione w następnym wydaniu biuletynu, tak aby był on nie tylko zbiorczym źródłem informacji dla dużej grupy osób, ale także stymulowałby dalsze pytania. Dać przykład:

Pytanie: Czasami znajduję się w sytuacjach, które nie zostały omówione w żadnej z prezentacji Security ASwareness lub wspomniane konkretnie w polityce bezpieczeństwa. Zgodnie z polisą kontaktuję się z działem IT lub działem bezpieczeństwa, aby dowiedzieć się, co dalej robić, ale obawiam się, że mogę się z nimi kontaktować z nieistotnymi lub głupimi pytaniami. Nie chcę im przeszkadzać ciągle z moimi problemami. Co powinienem zrobić i jak mam postępować?

Odpowiedź: Biuro Bezpieczeństwa Informacji (ISO) ma obowiązek odpowiadać na każdy e-mail dotyczący bezpieczeństwa firmy, a także obsługi korespondencji dotyczącej potencjalnych problemów z bezpieczeństwem itp. Ich funkcją jest nie tylko utrzymanie akceptowalnego poziomu bezpieczeństwa firmy ale także do szkolenia, edukowania i wspierania użytkowników. Niezależnie od tego, czy jest jakieś zdarzenie, problem lub coś, na co nie masz pewności, jesteś wezwany do skontaktowania się z biurem ISO na 123-456-789 w pilnych sprawach, lub w przypadku braku pilności, napisz do nas linijkę używając naszego adres e-mail, security@company.com.

Pamiętaj, aby nie działać w oparciu o coś, czego nie jesteś w 100% pewny, i pamiętaj, że nie ma czegoś takiego jak "kłopotać się", jeśli chodzi o zabezpieczenie zasobów informacyjnych firmy. Dołącz do trzech pytań i odpowiedzi w każdym wydaniu; Pomoże to wielu osobom, a także pomoże w analizie skuteczności polityki bezpieczeństwa. Na podstawie zadanych pytań będziesz w stanie ustalić jeśli czegoś brakuje lub nie jest w porządku, lub z drugiej strony może to również oznaczać, że zainteresowałeś ich i zmotywowałeś do uczenia się i zadawania dodatkowych pytań.

5 - Zasoby bezpieczeństwa

Ta sekcja może składać się z jednego lub dwóch krótkich wiadomości dotyczących aspektu bezpieczeństwa informacji w łatwy do zrozumienia sposób. Chodzi o to, aby pomóc użytkownikom zrozumieć znaczenie całego procesu zwanego przez nich szkoleniem w zakresie świadomości bezpieczeństwa, za pośrednictwem wiadomości dotyczących bezpieczeństwa, wiadomości o najnowszych naruszeniach bezpieczeństwa, stratach ponoszone przez firmy z powodu problemów z

bezpieczeństwem itp. Kolejnym cennym zasobem, który możesz chcieć uwzględnić, są linki do stron zewnętrznych kierowanych do osób, które nie są zainteresowane tematem (często określani jako początkujący lub neofici) i dobrze znane fora bezpieczeństwa moderowane przez szanowanych ekspertów ds. bezpieczeństwa. Przed połączeniem z jakąkolwiek witryną, musisz w pełni przejrzeć jej zawartość i oszacować, jak użyteczna (jeśli w ogóle) jej zawartość byłaby dla użytkowników, którzy chcą uzyskać informacje z zewnętrznych źródeł.

6 - Kontakt

Należy pamiętać o podaniu danych kontaktowych biura ISO na początku i na końcu każdego wydania, aby użytkownicy wiedzieli dokładnie, z kim skontaktować się w przypadku problemu.

Kontakty Biura Bezpieczeństwa Informacji:

http://company.com/security/

email: security@company.com

telefon: 123-456-789

987-654-321 Zewn. 000

Zalecenia dotyczące biuletynu bezpieczeństwa

Ta sekcja ma na celu przedstawienie pewnych zaleceń dotyczących biuletynu dotyczącego bezpieczeństwa, aby pomóc Ci w różnych tematach od udanej implementacji do poprawy jej ogólnej skuteczności. Przede wszystkim należy zarchiwizować wszystkie poprzednie wydania biuletynu bezpieczeństwa w intranecie firmy, aby personel mógł uzyskać dostęp do wszystkich problemów; możesz również rozważyć umieszczenie archiwum na zewnętrznej stronie internetowej, ale zależy to oczywiście od wrażliwości publikowanych informacji na zewnątrz.

Opublikuj biuletyn o bezpieczeństwie co tydzień lub dwa razy w miesiącu w zależności od częstotliwości sesji Security Awareness. Zachowaj krótkie i krótkie artykuły i staraj się nie podawać zbyt wielu informacji technicznych; kluczową zasadą jest informowanie i edukowanie, a nie przeciążanie ich nadmiernymi informacjami.

Reklamuj, jeśli ludzie nie wiedzą o istnieniu biuletynu lub nie wiedzą o tym ale nie dbają o niego ,ważne, że będą go czytać. Przesyłaj biuletyn w sesjach świadomości, dołączaj informacje o nim do innych e-maili, umieszczaj je na plakatach, włączaj do innych wewnętrznych programów i kampanii w firmie, reklamuj w firmowym intranecie.

Zawsze angażuj ludzi; im bardziej ludzie czują się zaangażowani lub czują, że mogą wnieść swój wkład, tym większe zainteresowanie i pasja będą mieli w temacie. Pomoże to również "rozpowszechnić wiadomości" wśród pracowników, co może również zwiększyć dodatkowe zainteresowanie. Poproś o opinie, abyś mógł monitorować, co się dzieje. Jak wspomniano wcześniej, pomoże to nie tylko w poprawieniu treści biuletynu, jeśli zajdzie taka potrzeba, ale także w ocenie ogólnego sukcesu.

Witryna internetowa poświęcona bezpieczeństwu informacji

Zaleca się utworzenie witryny internetowej dotyczącej bezpieczeństwa informacji, która będzie głównym punktem wyjścia dla wszystkich zainteresowanych bezpieczeństwem IT. Jeśli z powodzeniem wdrożone, przedsięwzięcie to stworzy poczucie wspólnoty na dłuższą metę, co jest nieocenionym atutem dla bezpieczeństwa firmy w ogóle. Na tym etapie musisz zdecydować, czy ta strona internetowa ma być całkowicie oddzielną, niezależną witryną lub podzbiorem, czy też dodatkiem do

istniejącego intranetu firmowego. W niektórych ekstremalnych przypadkach możesz również rozważyć utworzenie dwóch oddzielnych witryn; strona wewnętrzna, tylko dla pracowników (i dostępna tylko z sieci firmowej) i strona zewnętrzna, dostępna dla wszystkich na całym świecie, a także dla personelu, na przykład podczas przeglądania Internetu z domu. Są oczywiście różne opcje i punkty do przemyślenia tutaj, na przykład, czy chcesz, aby były dostępne dla wszystkich, czy chcesz je zabezpieczyć hasłem i / lub umieścić na określonym porcie serwera, czy zawartość zewnętrznego strona (extranet) może być widoczna lub opublikowana w świecie zewnętrznym, konserwacja systemów i treści itp., dlatego zaleciłbym, aby wszystko było tak proste, jak to tylko możliwe. Witryna musi być przejrzysta, łatwa do przeglądania i łatwa w nawigacji; nie przeładowuj go tysiącami plików i dokumentami technicznymi, z których większość prawdopodobnie zawiera słowa nieznane członkom personelu. Przekaż im konkretne artykuły napisane przez biuro ISO na temat najczęstszych problemów związanych z bezpieczeństwem, z jakimi mogą się spotkać podczas korzystania z systemów firmowych i obsługi poufnych danych, ucz ich jak identyfikować problemy, zgłaszać i radzić sobie z incydentami. Dostarcz im interesujące i wyczerpujące odpowiedzi na najczęściej zadawane pytania; jeśli nie możesz znaleźć odpowiedniej treści do swoich potrzeb, napisz nowe i rozpowszechniaj je wśród pracowników korzystających z witryny internetowej poświęconej bezpieczeństwu jako medium dystrybucji. Zawarliśmy kilka linków do zewnętrznych stron internetowych, na których będzie można zobaczyć kilka przykładów, które, mam nadzieję, zaoszczędzą sporo czasu i badań.

Technika "Potrzebujemy CIEBIE"

Jest to technika obowiązkowa, jeśli chodzi o zmianę podejścia pracowników do ich roli w bezpieczeństwie firmy. Zasadniczo zapewnia wszystkim zaangażowanym możliwość aktywnego udziału w procesie edukacyjnym za pomocą własnych porad, pomysłów, osobistych doświadczeń, zaleceń itp. a jeśli są wystarczająco dobre, pracownik otrzyma możliwość osobistego przedstawienia tematu na jednym z wykładów lub dyskusji. Ta metoda zmotywuje mniej lub bardziej wszystkich do udziału w programie uświadamiającym bezpieczeństwo, a z drugiej strony stworzy bardziej przyjazną, bardziej nieformalną atmosferę. Posiadanie współpracownika zwracającego się do nich ich poglądami znacznie zmniejszy stres i formalność procesu edukacyjnego. Każdy może wysyłać sugestie i zalecenia do programu, ponieważ aktywnie angażuje pracowników w ten proces i pomaga zmienić sposób myślenia. Nie postrzegają edukacji bezpieczeństwa jedynie jako zobowiązania tylko dlatego, że są na liście płac, ale aktywną kwestią dotyczącą dobra całej instytucji. Jako dodatkowy bonus dowiedzą się również, jak chronić swój osobisty komputer w domu i zbierać cenne wskazówki i wskazówki.

Konkursy edukacyjne

Prowadzenie różnych konkursów związanych z bezpieczeństwem od czasu do czasu pomaga nie tylko zmierzyć poziom świadomości personelu w zakresie bezpieczeństwa, ale także zmienia i wprowadza innowacje w procesie edukacyjnym. Konkursy na łamanie haseł są dobrym przykładem; uczestnicy stają przed wyzwaniem złamania pliku, który był chroniony hasłem wybranym przez innego uczestnika, z ideą znalezienia / wyeliminowania słabego hasła. Po zakończeniu konkursu rozpoczyna się dyskusja na temat sposobu złamania hasła, co czyni go słabym hasłem (jeśli tak było) itp. Większość pracowników jest zwykle zainteresowana takimi działaniami, a większość z nich zrobi wszystko, aby używaj trudnych do złamania haseł zgodnie z zaleceniami dotyczącymi procesu tworzenia silnych haseł z kursu Security Awareness Course.

16. Podsumowanie zarządzania

Ta sekcja została stworzona głównie z myślą o odpowiedzi na najczęściej zadawane przez kierownika pytania dotyczące bezpieczeństwa informacji. Jego celem jest krótkie, ale skuteczne wyjaśnienie, dlaczego z punktu widzenia zarządzania chciałoby się zainwestować w zabezpieczenie podstawowych

zasobów informacyjnych firmy, a także potencjalnych zagrożeń związanych z cięciem budżetu na bezpieczeństwo informacji. Wiele firm (wciąż) zwykle zadaje sobie pytanie, dlaczego powinny inwestować w bezpieczeństwo informacji, ponieważ poufne dane są codziennie archiwizowane, a w przypadku włamania, epidemii wirusów lub uszkodzenia danych, procesy informacyjne i biznesowe mogą zostać przywrócone i wprowadzone w życie. z powrotem w ciągu kilku minut. Podczas gdy teoretycznie nie ma nic złego w tym sposobie myślenia i procedurach, które są na miejscu zapewniając pewien stopień bezpieczeństwa, praktyka wykazała raz za razem, że "klasyczne" metody bezpieczeństwa, takie jak skaner antywirusowy / tworzenie kopii zapasowych / przywracanie, mogą nie wystarczyć do "utrzymania fortu". Ludzie wciąż nie zdają sobie sprawy, że ich łączność z Internetem stanowi duże zagrożenie dla całego świata, jeśli nie jest odpowiednio zabezpieczona; że istnieje kod hybrydowy, który nie tylko usunie twoje sieci i wyrzuci twoje dane, ale także ukradnie dokumenty, hasła itp. i że są ludzie, którzy spróbują wejść do twojego systemu z dowolnego powodu i uszkodzić twoje systemy. Pomyślne wtargnięcie w ideę celowego wyrządzania szkód w biznesie może zniszczyć wizerunek firmy i nazwy marki bez końca. Odzyskanie uszkodzonych plików może potrwać kilka minut, ale usunięcie nazwy lub zdjęcia może potrwać lata. Proste zlikwidowanie strony internetowej firmy pokaże światu, jak niepewne jest to (a następnie systemy wewnętrzne), że nie zastosowano właściwych środków bezpieczeństwa, a jeśli chodzi o sklep internetowy, większość klientów będzie bać się go już używać. Albo wyobraź sobie, że sieci Twojej firmy przyczyniają się do przeprowadzenia ataku DDoS (Distributed Denial Of Service) na całym świecie, który z pewnością wpędzi cię w kłopoty i / lub bardzo zaszkodzi twojej reputacji. Wyobraź sobie, że znajdujesz się w sytuacji, w której Twoje systemy firmy nieświadomie atakują inne firmy online lub przeprowadzane są udane penetracje w innych firmach, korzystając z twoich sieci! Innym częstym błędem w zarządzaniu jest zwykły i prosty, zadowolony z siebie Dział IT Ile razy słyszałeś frazy typu: "niedawno zakupiliśmy dobrze znany produkt firewall, aby chronić sieć naszej firmy", "mamy również oprogramowanie blokujące treści na poziomie serwera", "nasz administrator jest certyfikowanym specjalistą od zabezpieczeń" lub " uważamy, że jesteśmy bezpieczni, więc dlaczego mielibyśmy inwestować w dalsze środki bezpieczeństwa? ". Bezpieczeństwo to niekończący się proces, który wymaga stałego monitorowania, aktualizacji, inwestycji, badań i wdrażania nowych technologii; nie zapominając o najważniejszym punkcie: edukacja personelu. Ponieważ bez względu na to, ile pieniędzy jesteś gotów wydać, bez względu na zastosowane technologie, sekret leży w osobie, która konfiguruje twoje systemy bezpieczeństwa. Internet może być bardzo korzystnym zasobem dla Twojej firmy, ale wiąże się z nim pewne ryzyko. Aby uzyskać najlepsze możliwe wyniki, prawdopodobnie będziesz musiał zatrudniać pełnoetatowych specjalistów zajmujących się bezpieczeństwem (IT), zapewniając w ten sposób czerpanie korzyści z Internetu, przy rozsądnym zabezpieczeniu ważnych danych. Należy mieć nadzieję, że do tej pory każdy menedżer firmy ma wystarczającą ilość informacji ogólnych, aby móc zadawać właściwe pytania swoim dostawcom produktów zabezpieczających lub firmom zajmującym się doradztwem bezpieczeństwa, budując i rozwijając swoje rozwiązania bezpieczeństwa. Z drugiej strony mogę podkreślić, że ważne jest, aby kierownictwo firmy zostało zaznajomione ze wszystkimi zagrożeniami związanymi z łącznością internetową i innymi problemami związanymi z bezpieczeństwem; Bardziej zdecydowani menedżerowie i decydenci najwyższego szczebla z całą pewnością znajdą się w sytuacji z punktu widzenia bezpieczeństwa, tym szybciej i szybciej zostanie wprowadzona skuteczna polityka / strategia bezpieczeństwa IT.